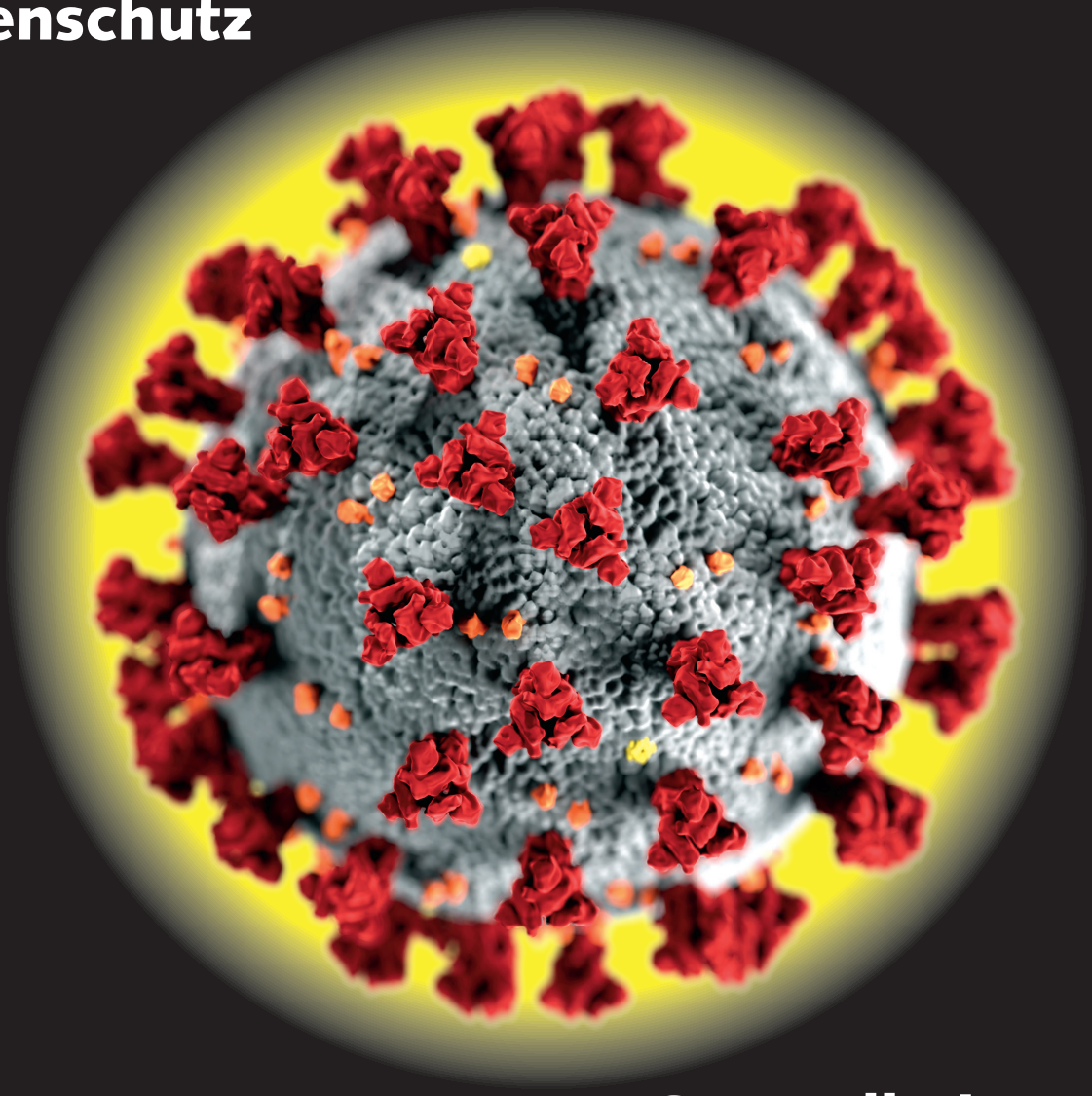
H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

37. Jahrgang 2020 Einzelpreis: 7 EUR 2/2020 – Juni 2020

Corona und der Datenschutz



Gesundheitswesen im Datenrausch

ISSN 0938-3476

• Grundrechte • Gender • Individualisierte Propaganda • Netzpolitik.org •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Inhalt

Ausgabe 2/2020

inhalt

Titelbild: https://commons.wikimedia.org/wiki/File:SARS-CoV-2_without_background.png

Schwerpunkt „Gesundheitswesen im Datenrausch“

Netzpolitik.org

Lesen & Sehen

Editorial

Großen Raum nehmen in dieser Ausgabe der *FIfF-Kommunikation* Themen ein, die sich um unsere Gesundheit drehen. Neben dem bereits lange geplanten Schwerpunkt *Gesundheitswesen im Datenrausch* ist dies das *Corona-Virus* SARS-CoV-2, die dadurch ausgelöste Pandemie und deren Folgen für Grundrechte und Digitalisierung.

Der Schwerpunkt setzt sich aus unterschiedlichen Perspektiven in fünf Beiträgen mit der Digitalisierung des Gesundheitswesens und den damit verbundenen Risiken auseinander. Im eigenen Schwerpunkteditorial heißt es dazu:

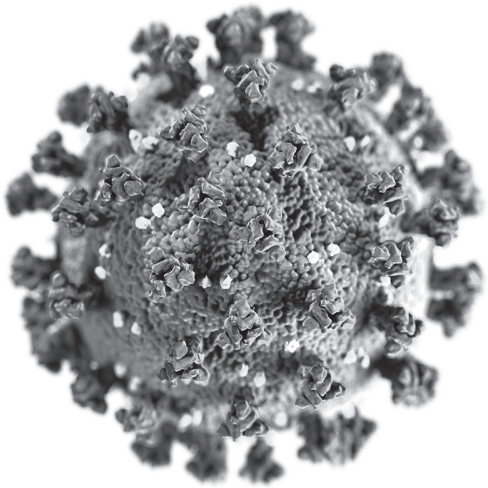
> *„Seit mehr als 20 Jahren verfolgt die Bundesregierung – völlig unbeeinflusst von der unterschiedlich geprägten parteipolitischen Zusammensetzung der jeweiligen Regierungskoalition – einen Kurs der Digitalisierung und Technisierung des öffentlichen Gesundheitswesens, mittlerweile häufig auch ‚Gesundheitswirtschaft' genannt. … Von Beginn an war die Digitalisierung und Technisierung des öffentlichen Gesundheitswesens auch Gegenstand der Kritik …"*

Der Schwerpunkt geht auf eine Initiative von *Arne Buß* zurück. Das FIfF dankt Arne für die aktive Unterstützung bei der Gewinnung der AutorInnen.

Die Corona-Pandemie und ihre Auswirkungen in Form von Abstandsregeln und Kontaktsperren haben die Digitalisierung unserer Gesellschaft vielleicht stärker vorangetrieben als manche politischen Programme. Mobiles Arbeiten hat auch dort Einzug gehalten, wo ihm vorher mit Zurückhaltung begegnet worden war: Das Arbeiten von zu Hause ist gerade weit verbreitet – zumindest dann, wenn es die Natur der Tätigkeiten erlaubt. Gleichzeitig sollen technische Lösungen eingesetzt werden, um die Entwicklung der Pandemie zu verfolgen und ihre Auswirkungen einzudämmen. Eine *Corona-App* soll dies bewerkstelligen – dahinter verbirgt sich ein ganzes Bündel von Zielsetzungen und technischen Konzepten: Soll die App dazu beitragen, Infektionsketten nachzuverfolgen – personalisiert, pseudonym oder anonym? Soll sie Menschen warnen, wenn sie einem erhöhten Ansteckungsrisiko ausgesetzt waren und ein Test auf das Virus erfolgen sollte? Soll sie gar die Bewegung Infizierter überwachen, ähnlich einer elektronischen Fußfessel? Und wie soll das technisch umgesetzt werden: mit zentraler Datenspeicherung oder dezentral?

Die Diskussionen zeigen, dass es von der schlichten Forderung: „Wir brauchen eine App!" bis zur Klärung, was eigentlich damit erreicht werden soll, ein längerer Weg werden kann. Das beginnt bereits damit, dass offenbar nicht einmal ein einheitliches Verständnis von Datenschutz zugrundegelegt wird. Auch dürfen wir nicht in einen *Solutionismus* verfallen, der für jedes Problem an eine technische Lösung glaubt. Nach längerer Diskussion steht nun die individuelle Warnung vor einem Infektionsrisiko im Vordergrund.

Zur Corona-App haben *Kirsten Bock*, *Christian Ricardo Kühne*, *Rainer Mühlhoff*, *Měto R. Ost*, *Jörg Pohle* und *Rainer Rehak* Pionierarbeit geleistet: Sie haben eine *Datenschutz-Folgenabschätzung* für eine – zu diesem Zeitpunkt noch hypothetische – Corona-App erarbeitet, die auch in der Fachwelt auf einiges Interesse stößt. Diese Ausgabe enthält eine zusammenfassende Stellungnahme, die Geschichte, wie es dazu kam und die aus der Analyse abgeleiteten Empfehlungen. Weitere Stellungnahmen aus der Zivilgesellschaft, die auch bei notwendigen Maßnahmen in der Krise die Wahrung der Grund- und Menschenrechte fordern, schließen sich an. „Grundrechte gehören nicht in Quarantäne!", betont beispielsweise die *Humanistische Union*. Auch in unserer Rubrik *Netzpolitik.org* nehmen diese Themen breiten Raum ein, beispielsweise zur Überwachung, zur Krise als Hebel für Grundrechtseinschränkungen, aber auch zur Situation des digitalisierten Schulunterrichts in Zeiten von Corona.



Von einem Projekt, das Unterrichtsmaterialien zur Vermittlung von Gender-Wissen und Gender-Kompetenzen anbietet, berichtet *Göde Both*. Das Portal *Gendering MINT digital* ist am Zentrum für transdisziplinäre Geschlechterstudien (ZtG) an der Humboldt-Universität zu Berlin angesiedelt. Die verfügbaren *Open Educational Resources* basieren auf den Ergebnissen von mehr als 40 Jahren Forschung und Lehre.

Social Media und die Möglichkeiten gesetzlicher Kontrolle untersucht *Dominik Wetzel* in seinem Beitrag *Individualisierte Propaganda*. Ausgangspunkt ist die extreme Reichweite, die diese Medien inzwischen haben:

> *„Das ist gefährlich, wie der Fall um Cambridge Analytica zeigt. Mithilfe von Algorithmen war es möglich, unzählige Persönlichkeitsprofile zu sammeln, um den Nutzerinnen und Nutzern zugeschnittene Informationen zukommen zulassen, die ihr Bild von der Wirklichkeit beliebig beeinflussen konnten."*

Der Autor analysiert die Risiken durch Beeinflussung der NutzerInnen und für die freie Meinungsäußerung, und untersucht mögliche Gegenmaßnahmen. Er fordert, die informationelle Selbstbestimmung auch gegenüber Privatunternehmen aufrecht zu erhalten und neue Strukturen zu schaffen, die Erstellung und Handel mit psychologischen Profilen von Kunden verhindern.

Die Ausgabe wird ergänzt durch zwei kurze Artikel in eigener Sache: Im wissenschaftlichen Beirat des FIfF begrüßen wir

Dietrich Meyer-Ebrecht, *Eberhard Zehendner* und *Benjamin Kees* als neue Mitglieder. Der zweite Beitrag – der SchlussFIfF – zeigt, wie stark auch das FIfF durch die Corona-Pandemie betroffen ist: Wir werden unsere diesjährige Konferenz erstmals nicht vor Ort, sondern digitalisiert organisieren. So sehr wir bedauern, dass wir uns im November nicht in Weimar treffen können, so sehr freuen wir uns auf die Chancen der Digitalisierung auch für die Arbeit des FIfF.

Bekanntlich gibt das FIfF nicht nur die *FIfF-Kommunikation* heraus, sondern ist auch an weiteren Publikationen beteiligt. Der *Grundrechte-Report 2020* wurde am 2. Juni 2020 vorgestellt; die Aufzeichnung ist auf unserer Webseite zu finden. Eure solidarische Unterstützung benötigt die Zeitschrift *Wissenschaft & Frieden*; Näheres dazu findet Ihr im Heft.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion

Der Brief

Corona

Liebe Freundinnen und Freunde, liebe Mitglieder des FIfF,

eine humoristisch gemeinte Umfrage, wer in einem Unternehmen am meisten zur Digitalisierung beigetragen habe – CIO, CDO oder COVID-19; angekreuzt war COVID-19 – zeigt, welchen Einfluss die Krise, auch im positiven Sinne, haben kann, und dass Veränderungen, die bis vor Kurzem unmöglich schienen, unter dem aktuellen Handlungsdruck sehr schnell umgesetzt werden.

Es ist also wohl zu erwarten, dass die Krise sich auch langfristig auf unser Leben auswirken wird, positiv wie negativ. Es sind besonders drei Entwicklungen, die auf unser tägliches Leben im unmittelbaren Umfeld einen Einfluss haben und auf die Bedrohung durch den Corona-Virus zurückgehen:

- Eingriffe in das öffentliche Leben: Kontaktverbote, Ausgangssperren, Reisebeschränkungen und Einschränkungen des Wirtschaftslebens waren bis vor Kurzem in Friedenszeiten undenkbar. Dennoch treffen sie offenbar auf eine hohe Akzeptanz in der Bevölkerung. Die Frage ist, welche Lehren daraus gezogen werden – nicht zuletzt durch die Auswirkungen des Klimawandels ist künftig vielleicht häufiger mit solch einschneidenden Maßnahmen zu rechnen.

- Überwachung: Über eine *Corona-App* wird heftig diskutiert.[1] Sie soll Infektionsketten nachvollziehbar machen und damit wichtige Erkenntnisse für die Bekämpfung der Pandemie liefern. Unterschiedliche Konzepte bieten dabei ein unterschiedliches Datenschutzniveau. Bevor man über Datenschutz debattiert, sollte aber geprüft werden, ob die Konzepte überhaupt das erfüllen, was von ihnen erwartet wird. Soziale Probleme mit rein technischen Mitteln lösen zu wollen, wird auch hier nicht funktionieren.[2] Nicht zu vergessen sind die Nebeneffekte, etwa die Schaffung von Akzeptanz und die Gewöhnung an alltägliche Überwachung.

- Mobiles Arbeiten: Viele Arbeitgeber waren bisher zögerlich, wenn es um die Einführung von mobilem Arbeiten und Home-Office-Konzepten ging – auch dann, wenn die Natur der Tätigkeiten dies prinzipiell erlaubte. Nun wird es im Verlauf der Krise massiv ausgebaut – zunächst eine positive Entwicklung. Doch langfristig müssen jetzt auch die notwendigen Infrastrukturen geschaffen werden. Nicht alle ArbeitnehmerInnen können in ihren Wohnungen einen Arbeitsplatz einrichten, der den Anforderungen an konzentriertes Arbeiten, Arbeitssicherheit, Ergonomie und Informationssicherheit genügt. Ähnlich gilt das für die Bildung. Der Anlauf, auch den Schulunterricht nach Hause zu verlagern, hat auch unsere Defizite bei der Digitalisierung schonungslos offengelegt – nicht nur technisch, sondern auch sozial. *Digital divide* mitten in unserer Gesellschaft.

Wir sind also gerade dabei, vieles umzukrempeln, was uns bisher selbstverständlich war – ohne die Zeit dafür zu haben, die Veränderungen richtig vorzubereiten.

Dabei geht es nicht um ein naives „Digital first, (Be-) Denken second." Man darf auch nicht in einen ebenso naiven *Solutionismus*[3] verfallen, der für jedes Problem eine digitale Lösung erwartet. Gerade beim FIfF wissen wir, dass soziale Probleme in der Regel nicht technisch lösbar sind. Stets gilt es, Chancen und Risiken abzuwägen um zu sinnvollen Lösungen zu kommen. Vielleicht hat aber nicht zuletzt auch eine gewisse Zögerlichkeit in der Anwendung digitaler Lösungen mit dazu geführt, dass wir uns heute einem Oligopol internationaler Großunternehmen gegenübersehen, die den Markt und die Anwendungen bestimmen.

Die Welt *nach Corona* wird wohl nicht mehr die gleiche sein, wie davor. Wichtig ist, dass wir die richtigen Schlüsse und Folgerungen daraus ziehen: Wie helfen wir unserer Wirtschaft wieder auf die Beine? Wie können wir den Stillstand überwinden und wie können wir den Unternehmen und Menschen helfen, aus der Krise herauszukommen.

Doch wie können wir eine nachhaltige und resiliente Wirtschaft schaffen? Eine Wirtschaft, die nicht bei jeder Krise sofort zu chaotischen Zuständen führt?[4] So ist der Klimawandel, durch das Corona-Virus nicht verschwunden.[5] Gerade wurde über staatliche Subventionen für den Autokauf diskutiert, eine „Abwrackprämie 2.0", sozusagen. Die Fußball-Bundesliga sollte möglichst schnell wieder starten – auch ohne Zuschauerinnen und Zuschauer (bisher hatte ich gedacht, dass diese bei Unterhaltungs-

betrieben wie der Fußball-Industrie irgendwie wichtig sind). Warum wir unser (Steuer-) Geld nach überstandener Pandemie ausgerechnet für Fußball und ein neues Auto ausgeben sollen, anstatt, sagen wir mal, für eine Verbesserung der Bildung gerade jetzt im digitalen Raum zu sorgen, müssten die Protagonisten solcher Ideen mal genauer erklären. Gerade die Subventionierung des Verbrennungsmotors – immer noch indirekt, über die Senkung der Mehrwertsteuer – mag wirtschaftlich kurzfristig Sinn ergeben – umweltpolitisch ist es mehr als fragwürdig. Haben wir die verheerenden Waldbrände in Australien schon vergessen? Was wir brauchen, sind zukunftsfähige Mobilitätskonzepte. Die Corona-Krise ist vielleicht nur ein vergleichsweise harmloser Anfang dessen, was uns noch erwartet, wenn der Klimawandel sich beschleunigt und die Auswirkungen immer spürbarer werden. Und: Beim Klimawandel können wir nicht auf einen Impfstoff hoffen, nach dessen Entwicklung alles vorbei ist.

Diejenigen, die gerne in die 1950er und 1960er Jahre zurück möchten, wollen auch diese Krise nicht wahrhaben. Verschwörungstheorien blühen. *Wir sollen zu Hause bleiben, damit unbemerkt Flüchtlinge in Land geschafft werden können.* Manchmal könnten solche Verschwörungstheorien fast zum Lachen sein, hätten sie nicht ernstzunehmende Konsequenzen.[6]

Aber Achtung! In den letzten Wochen wurden ja tatsächlich unsere Grundrechte massiv eingeschränkt. Grundrechte sind keine Schönwetterrechte, sie sind in der Krise besonders wichtig. Wer sie – auch temporär – einschränkt, muss diese Einschränkung rechtfertigen und sie sofort zurücknehmen, wenn der Grund dafür entfallen ist.[7] Viele von uns haben großes Verständnis für die Einschränkungen. Das mag in der Krisensituation richtig und sinnvoll sein – manchmal erscheint es mir aber fast schon zu eilfertig. Wir müssen auch in der aktuellen Situation kritisch bleiben. Was auch aus den Einschränkungen werden kann, zeigt sich gerade direkt vor – nein, nicht vor, schon hinter unserer europäischen Haustür: in Ungarn.

Über die Einschränkungen muss diskutiert werden – aber mit vernünftigen wissenschaftlichen und politischen Argumenten, nicht mit unhinterfragten Geschichten, unbegründeten Emotionen und Spinnereien. Dass sich wissenschaftliche Erkenntnisse und ihre Rahmenbedingungen auch einmal ändern, müssen wir aushalten. Hier sollten auch die Medien dazu beitragen, zu einem geordneten Diskurs zurückzufinden.

Die Reaktionen der zuständigen Behörden zeigen, dass vernünftige Argumente auch etwas bewirken, siehe zum Beispiel die Debatte über die Corona-App. Dass ein demokratischer Diskurs nicht immer zum schnellsten Ergebnis führt, liegt wohl in der Natur der Sache. Aber er führt meistens zu einem besseren Ergebnis. Gerade die Corona-App kann nur Nutzen stiften, wenn die Menschen ihre Nutzung nicht ablehnen.

Nein, das Corona-Virus ist keine Erfindung der Mächtigen, um uns künftig noch mehr zu knechten. Wir dürfen aber wohl davon ausgehen, dass die zuständigen Behörden genau beobachten und auswerten werden, wie die Krise verläuft und wie sich die Menschen verhalten. Und sehr wahrscheinlich werden sie daraus auch Erkenntnisse über die Steuerung der Bevölkerung – beispielsweise durch *Nudging* – und Gewöhnungseffekte allgegenwärtiger und akzeptierter Überwachung gewinnen.

Etwas merkwürdig scheint mir der Verlauf der politischen Debatte. Als erstes wäre doch zu erwarten, dass über die Maßnahmen, ihre Wirksamkeit und ihre Rahmenbedingungen berichtet wird. Gerne mischt sich darunter aber leider auch eine Form des Journalismus, der sich weniger für politische Inhalte interessiert als dafür, wer in einer Debatte *gewonnen* hat, ein wenig wie bei der Sportberichterstattung. Hat sich Angela Merkel durchgesetzt oder Armin Laschet? Wird Markus Söder jetzt der neue Bundeskanzler? Und wo sind eigentlich die SPD-Vorsitzenden? Es wird beklagt, dass sich die Ministerpräsidentinnen und Ministerpräsidenten der Länder nicht auf gemeinsame Regelungen einigen. Wie sind wir eigentlich Exportweltmeister geworden, wenn wir schon damit überfordert sind, dass in Berchtesgaden andere Ausgangsregelungen gelten als in Westerland oder in Görlitz?

Bei den benachbarten Großstädten Karlsruhe und Strasbourg stört es uns nicht. So stark ist unser Denken immer noch durch nationale Abgrenzung geprägt. Nach jahrzehntelanger europäischer Einigung fällt uns in der Krise als erstes ein, die Grenzen zu schließen. Sogar zwischen Bundesländern, womit wir wieder auf dem Stand des 19. Jahrhunderts angelangt wären.

Gefährlich wird es, wenn sich Verschwörungstheoretiker und rechte Spinner die verbreitete Unzufriedenheit mit den einschneidenden Maßnahmen zunutze machen, um ihre politischen Ziele durchzusetzen. Aber auch Leichtsinn nach dem Motto: „Es ist ja kaum etwas passiert, deswegen waren die Maßnahmen überzogen“, kann zum Problem werden.

Zurück zur Digitalisierung. FIfF-Vorstandssitzungen führen wir inzwischen selbstverständlich als Videokonferenz durch. Viele von uns arbeiten seit Wochen mobil von zu Hause aus – und es funktioniert. Das wird die Krise überdauern – aber nicht für alle. Wer diese Möglichkeit hat, dem sollten die damit verbundenen Privilegien bewusst sein – der Verkäufer im Supermarkt und die Friseurin können es nicht. Vor allem müssen wir auch bei digitalem Arbeiten Standards einhalten, die die Arbeitnehmer und allgemein die Nutzer der Technik schützen. Das beginnt mit der Umsetzung angemessener Datenschutzstandards nach DSGVO, geht aber noch weiter: Auch die IT-Sicherheit bei der Arbeit außerhalb der geschützten Sphäre des Büros ist ein Thema. Mobile Arbeitsplätze müssen ergonomisch gestaltet sein – das ist nicht der Stuhl am Küchentisch und auch nicht das Sofa, auf dem man es sich, glaubt man der Werbung, beim mobilen Arbeiten gemütlich macht.

Dennoch: Selbst im Fernsehen hat sich eine Art *Home-Office-Ästhetik* herausgebildet, wunderbar überspitzt dargestellt in der *Anstalt*. Meistens mit Bücherregal im Hintergrund. Konferenzen, bei denen wir uns gern auch persönlich getroffen haben, werden in den virtuellen Raum verlagert. Auch wir werden die diesjährige FIfF-Konferenz, die in Weimar geplant war, als Videokonferenz veranstalten.

Eins zuletzt, weil es so erbärmlich ist: Die Bundesrepublik Deutschland, einer der wohlhabendsten Staaten der Welt, hat aus dem Flüchtlingslager Moria auf Lesbos nach wochenlangem Gezerre nicht mal 50 Kinder gerettet, die dort unter menschenunwürdigen Bedingungen wochenlang hausen mussten[8]. Wow! Aber hey, die Spargelernte[9] ist gesichert.

Mit FIfFigen Grüßen

Stefan Hügel

Anmerkungen

1 *Bock K, Kühne CR, Mühlhoff R, Ost MR, Pohle J, Rehak R (2020) Datenschutz-Folgenabschätzung für die Corona-App, FIfF e. V.*

2 *Sehr skeptisch dazu Bruce Schneier: „My problem with contact tracing apps is that they have absolutely no value … to me, it's just techies doing techie things because they don't know what else to do." Schneier B (2020) Me on COVID-19 Contact Tracing Apps, Schneier on Security, https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html*

3 *Morozov E (2013) To save everything, click here. The Folly of Technological Solutionism, New York*

4 *Nuss S (2020) Geld oder Leben. Corona und die Verwundbarkeit der Eigentumslosen. PROKLA Zeitschrift für kritische Sozialwissenschaft, Band 50 Ausgabe 2 (199), Juni 2020, S. 201-218*

5 *Götze-Riccieri S (2020) Corona: Feuerprobe für den Klimaschutz.Blätter für deutsche und internationale Politik 6'20, Juli 2020, S. 29-32*

6 *Nocun K, Lamberty P (2020) Fake Facts. Wie Verschwörungstheorien unser Denken bestimmen. Köln: Quadriga*

7 *Zu den Grundrechtseinschränkungen in Zeiten von Corona siehe auch FIfF e. V. (2020) in dieser Ausgabe der FIfF-Kommunikation, S. 15*

8 *Die Kapitulation des Innenministeriums vor der AfD. Tagesspiegel, https://www.tagesspiegel.de/politik/50-fluechtlingskinder-aus-lesbos-die-kapitulation-des-innenministeriums-vor-der-afd/25725914.html*

9 *Offenlegung: Ich mag Spargel. Aber irgendwie vergeht mir gerade der Appetit.*

FIfF e. V. – Stellungnahme

FIfF veröffentlicht Datenschutz-Folgenabschätzung (DSFA) für die Corona-App

14. April 2020 – „Es geht nicht um Privatsphäre, sondern es geht darum, eine Technik sozial beherrschbar zu machen." *Dieses Datenschutzverständnis von Wilhelm Steinmüller (1934–2013), Datenschutzpionier und langjähriges FIfF-Mitglied, möchten wir, eine Gruppe WissenschaftlerInnen und DatenschützerInnen im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V., wieder stark machen.*

Seit einigen Wochen kreist die Diskussion um die Eindämmung der Corona-Pandemie zunehmend um den Einsatz technischer Hilfsmittel. Es wird geplant, die Pandemie durch den Einsatz von Tracing-Apps für Smartphones einzudämmen. Diese Systeme sollen automatisiert die zwischenmenschlichen Kontakte aller NutzerInnen aufzeichnen und es so erlauben, die Infektionsketten des Virus schnell und effizient nachzuvollziehen, um möglicherweise exponierte Personen frühzeitig warnen und isolieren zu können.

Wir haben es angesichts der geplanten Corona-Tracing-Systeme mit einem gesellschaftlichen Großexperiment zur digitalen Verhaltenserfassung unter staatlicher Aufsicht in Europa zu tun. **Die europäische Datenschutzgrundverordnung (DSGVO) verpflichtet die BetreiberInnen umfangreicher Datenverarbeitungssysteme (zu denen auch ein Corona-Tracing-System zählen würde) zur Anfertigung einer Datenschutz-Folgenabschätzung (DSFA) im Falle eines hohen Risikos für die Grund- und Freiheitsrechte.** Hierbei handelt es sich um eine strukturierte Risikoanalyse, die mögliche grundrechtsrelevante Folgen einer Datenverarbeitung im Vorfeld identifiziert und bewertet.

Wirksamkeit und Folgen entsprechender Apps sind noch nicht absehbar und es ist davon auszugehen, dass innerhalb der EU verschiedene Varianten erprobt und evaluiert werden. Die datenschutz- und somit grundrechtsrelevanten Folgen dieses Unterfangens betreffen potenziell nicht nur Einzelpersonen, sondern die Gesellschaft als Ganze. Aus diesem Grunde ist nicht nur die Anfertigung einer DSFA angezeigt, sondern insbesondere auch ihre Veröffentlichung – und eine öffentliche Diskussion. Da bisher keine der beteiligten Stellen eine allgemein zugängliche DSFA präsentiert hat und selbst die vorgelegten *privacy impact assessments* unvollständig bleiben, **legen wir vom FIfF mit diesem Dokument eigeninitiativ eine solche Datenschutz-Folgenabschätzung als konstruktiven Diskussionsbeitrag vor.**

Zusammenfassung und Ergebnisse

1. Die in den Diskussionen vielfach betonte Freiwilligkeit der App-Nutzung ist eine Illusion. Es ist vorstellbar und wird auch bereits diskutiert, dass die Nutzung der App als Voraussetzung für die individuelle Lockerung der Ausgangsbeschränkungen gelten könnte. Das Vorzeigen der App könnte als Zugangsbarriere zu öffentlichen oder privaten Gebäuden, Räumen oder Veranstaltungen dienen. Denkbar ist, dass ArbeitgeberInnen solche Praktiken schnell adaptieren, weil sie mittels freiwillig umgesetzter Schutzmaßnahmen schneller ihre Betriebe wieder öffnen dürfen. Dieses Szenario bedeutet eine implizite Nötigung zur Nutzung der App und bedeutet erhebliche Ungleichbehandlung der Nicht-NutzerInnen. Weil nicht jede Person ein Smartphone besitzt, wäre hiermit auch eine Diskriminierung ohnehin schon benachteiligter Gruppen verbunden. Kirsten Bock vom FIfF kommentiert: „*Die Einwilligung ist nicht das richtige Regelungsinstrument für die Nutzung der Corona-App, weil deren Voraussetzungen nicht erfüllt sind. Der Gesetzgeber ist aufgerufen, das Nutzungsrisiko der App nicht auf die BürgerInnen abzuwälzen, sondern selbst die Voraussetzungen für eine freiwillige, sichere und grundrechtsverträgliche Lösung in einem Gesetz vorzugeben und die BürgerInnen so vor Grundrechtsverletzungen – auch durch Dritte – wirksam zu schützen.*" Martin Rost vom FIfF ergänzt prägnant: „*Von einer Einwilligung geht keine Schutzwirkung für Betroffene aus.*"

2. Ohne Intervenierbarkeit und enge Zweckbindung ist der Grundrechtsschutz gefährdet. So besteht ein hohes Risiko fälschlich registrierter Expositionsereignisse (falsch positiv), die zu unrecht auferlegte Selbst-Isolation oder Quarantäne zur Folge haben (zum Beispiel Kontaktmessung durch die Wand zwischen zwei Wohnungen). Um dem zu begegnen, bedarf es rechtlicher und faktischer Möglichkeiten zur effektiven Einflussnahme, etwa das Zurückrufen falscher Infektionsmeldungen, die

Löschung falsch registrierter Kontaktereignisse zu einer infizierten Person und das Anfechten von infolge der Datenverarbeitung auferlegter Beschränkungen. Eine solche Möglichkeit sieht bisher keines der vorgeschlagenen Systeme vor. „*Beim Datenschutz geht es genauso wenig um den Schutz von Daten, wie es beim Sonnenschutz um den Schutz der Sonne geht oder beim Katastrophenschutz um den Schutz von Katastrophen*“, spitzt Jörg Pohle vom FIfF zu.

3. Alle bislang erwähnten Verfahren verarbeiten personenbezogene Gesundheitsdaten. Das Verfahren besteht aus der Verarbeitung von Kontaktdaten auf den Smartphones, der Übermittlung dieser Daten auf einen Server nach der Diagnose einer Infektion und letztendlich deren Verteilung an alle anderen Smartphones zur Prüfung auf einen möglichen Kontakt mit Infizierten. Alle Daten auf einem Smartphone sind personenbezogen, nämlich bezogen auf die NutzerIn des Gerätes. Weil nur diejenigen Personen Daten übertragen, die als infiziert diagnostiziert wurden, sind die übertragenen Daten zugleich Gesundheitsdaten. Somit unterliegen diese dem Schutz der DSGVO.

4. Anonymität der NutzerInnen muss in einem Zusammenspiel rechtlicher, technischer und organisatorischer Maßnahmen erzwungen werden. Nur durch einen mehrdimensionalen Ansatz kann der Personenbezug wirksam und irreversibel von den verarbeiteten Daten abgetrennt werden, so dass danach von anonymen Daten gesprochen werden kann. Allen derzeit vorliegenden Vorschlägen fehlt es an einem solchen expliziten Trennungsvorgang. „*Wenn man sich hier nur auf technische Maßnahmen oder allein auf politische Beteuerungen verlässt, besteht ein großes Risiko der nachträglichen De-Anonymisierung*“, so Rainer Mühlhoff vom FIfF. Wir haben in dieser DSFA rechtliche, technische und organisatorische Anforderungen formuliert, deren Umsetzung in der Praxis eine wirksame und irreversible Trennung sicherstellen kann – nur unter diesen Voraussetzungen dürften die infektionsanzeigenden Daten ohne Personenbezug (iDoP) an alle Apps verbreitet werden.

Wesentliche Voraussetzung für Transparenz bezüglich der Umsetzung aller Datenschutz-Grundsätze nicht nur für Datenschutzaufsichtsbehörden, sondern gerade auch für die Betroffenen und die (Zivil-)Gesellschaft insgesamt, ist die quelloffene Entwicklung von Server und Apps nebst allen ihren Komponenten beispielsweise als freie Software. Nur so kann es gelingen, Vertrauen auch bei jenen zu erzeugen, die nicht alle informationstechnischen Details verstehen. Ergriffene Maßnahmen müssen immer aktiv prüfbar gemacht und sauber dokumentiert werden.

Abschluss

Datenschutzanalysen betrachten die gesamte Verarbeitung von Daten, nicht nur die dabei eingesetzten Apps. „*Die Grenzen der App sind nicht die Grenzen der Verarbeitung*“, erläutert Christian Ricardo Kühne vom FIfF. In der öffentlichen Diskussion und in den betrachteten App-Projekten wird Datenschutz nach wie vor auf den Schutz der Privatsphäre, also Geheimhaltung gegenüber BetreiberInnen und Dritten, und auf Aspekte der IT-Sicherheit wie Verschlüsselung reduziert. Mit dieser Verengung der Sichtweise kommen die erheblichen, gesellschaftlich wie politisch fundamentalen Risiken, die wir in dieser Folgeabschätzung aufzeigen, nicht nur nicht in den Blick – sie werden zum Teil sogar verschleiert. „*Aus dem Blickwinkel des Datenschutzes gehen die wesentlichen Risiken nicht von HackerInnen oder anderen BenutzerInnen aus, sondern von den BetreiberInnen des Datenverarbeitungssystems selbst*“, kommentiert abschließend Rainer Rehak, Vorstandsmitglied des FIfF.

Referenzen

Download der DSFA (Creative-Commons-Lizenz: Namensnennung, CC BY 4.0 Int.) unter https://www.fiff.de/dsfa-corona: Deutsch, Englisch, Spanisch (Solamente el resumen), Französisch (Seulement le résumé) in der jeweils aktuellen Fassung. Diskussion im FIfF-Github-Repositorium: https://github.com/fiff-de/dsfa-corona

Data Protection Risks of a Corona App: Full updated version of the Data Protection Impact Assessment (DPIA) now available in English

29th of April 2020 – *Doubts about usefulness of Corona App remain, even decentralised variants involve considerable risks – FIfF presents DPIA update in English at https://www.fiff.de/dsfa-corona*

The debate about the data protection-compliant design of a corona app has intensified in recent days. The app digitally supports the so called „contact tracing“ which intends to break COVID-19 infection chains by warning people who have been exposed to someone tested positive. Initially, the only goal pursued by the German government was to introduce an app with a warning functionality for those potentially infected, but in the meantime, further purposes beyond tracing are being discussed which would cause more infringements of fundamental rights. However, there are still general doubts about the effectiveness of digital contact tracing for containing the pandemic, as the discussion about false positives caused by e.g. walls, masks or varying Bluetooth signal strengths shows. The accusations that pushing such a corona app project primarily signals political actionism or that the project might accustom the general population to future tracing or tracking projects by government bodies have not yet been dispelled.

In the course of the current discussion about a ‚stay at home‘ order exit strategy, the use of a corona app has been considered strategic in other countries and is now also being considered by the German government. The German Minister of Health, Jens Spahn, has recently switched his preference from a centralized, and from a data protection point of view riskier architecture, to a decentralized model. Austria and Switzerland have already adopted the decentralized DP-3T implementation**. With the publication of a DPIA, we are pursuing the goal of informing the discussion about the far-reaching consequences of these decisions and contributing to making this app as data protection-friendly as possible.**

One of the central questions relevant to data protection is: How is the purpose limitation of the overall system secured and enforced? How can misuse, especially by the operators, be pre-

vented by technical, organizational, and legal means? It will be decisive for the success of a data protection-friendly Corona App to restrict the purpose solely to informing potentially infected persons. In our view adding other purposes such as epidemiological studies, an immunity pass function, or detailed quarantine monitoring poses disproportionate risks and infringements of fundamental rights and is therefore not justifiable.

The question of centralisation vs. decentralisation is of crucial importance for data protection due to the following circumstance: In a central architecture, an almost ‚omniscient' server coordinates all procedural activities; It collects all contact events from infected users and notifies persons at risk. In a decentralized architecture, however, the server has no access to the contact events of users. It only stores non-identifying infection indicating data. The apps themselves detect possible infection events; the necessary calculations are performed on the devices of the respective users. If a government agency were to be given blanket access to contact events of infected and non-infected persons, this would not only be a considerable violation of data protection, but also a collection of data that is simply not necessary for the purpose, i.e. a violation of the principle of data minimization. **„So far, the European Parliament, Germany, Austria, Ireland and Switzerland have spoken out in favour of a decentralised variant, whereas France still favours the centralised one. The FIfF would like to urgently point out the danger that a centralised system will be followed by extensive possibilities for subsequent use, which generates considerable potential for abuse."** warns Kirsten Bock from FIfF.

A decentralised model is clearly preferable to a centralised one, but it is also not free of serious data protection risks. Therefore, the FIfF now presents a model data protection impact assessment (DPIA) for decentralised architectures. In doing so we refer to a requirement under Art. 35 of the General Data Protection Regulation (GDPR), which is directed towards the future controller of such data processing. The purpose of this model DPIA is to demonstrate in a publicly accessible way the risks for data subjects. **„It needs to be underlined that the data protection risks also affect persons who do not use the app themselves",** says Rainer Mühlhoff, FIfF e. V. Furthermore, with this document we present recommendations for the (re)design of the app and the processing procedure as well as protective measures concerning a whole list of possible weaknesses and attacks.

„With this DPIA, we have set a new standard that others whose data processing creates high risks for fundamental rights and freedoms have to meet from now on." comments Rainer Rehak from FIfF. **„And we are also showing that DPIAs must be published as a matter of principle so that society can discuss these risks in an informed manner and exert pressure on those responsible to protect our fundamental rights when processing data,"** adds Jörg Pohle, also from FIfF.

With this DPIA, now completely available in English, we intend to enrich the pan-European discussion on data protection. Data protection, not privacy, is the guarantor for the protection of all fundamental rights in the digital age.

Kirsten Bock, Christian Ricardo Kühne, Rainer Mühlhoff, Měto R. Ost, Jörg Pohle, Rainer Rehak

Die Grenze der App ist nicht die Grenze der Verarbeitung

Warum eine Datenschutz-Folgenabschätzung zur *Corona-App* durch das FIfF erstellt wurde

Eine AutorInnengruppe aus FIfF-Mitgliedern hatte sich Anfang April gefunden, um Konzepte zum Contact-Tracing per App („Corona-App") *aus Datenschutzsicht zu untersuchen.*

Eigentlich kritisch gegenüber jeder Art von automatisierter Tracing-App eingestellt, nahmen sich die AutorInnen vor, Schadensbegrenzung zu betreiben. Wenn diese Apps also nicht mehr zu verhindern sind, dann sollte zumindest derjenige Typ von App stark gemacht werden, mit dem die geringste Eingriffsintensität in die Grundrechte der AnwenderInnen einherginge. Linus Neumann, einer der SprecherInnen des Chaos Computer Clubs, hatte auf seinem Blog drei Typen von Technologien für Contact-Tracing-Apps und ihren wesentlichen Eigenschaften unterschieden: GPS-Daten, Bewegungsdaten und Kontaktdaten. Besonders im asiatischen Raum wurden mitunter alle diese Daten ausgewertet, was aus Verhältnismäßigkeitsüberlegungen hierzulande ausscheidet.

Der Zweck eines Contact-Tracings soll, so bestimmte es diese AutorInnengruppe dann im Laufe ihrer Arbeit, einzig darin bestehen, Infektionsketten zu erkennen und diese zu unterbrechen. Dieser Funktionsumfang konnte mit den Typ-3-Daten, also *Kontaktdaten* am ehesten umgesetzt werden. Insbesondere fasste Neumann ein dezentrales Verfahren zusammen, welches im *WirVsVirus*-Hackathon entwickelt worden war. Zudem hatte eine internationale EntwicklerInnengruppe unter der Projektbezeichnung DP-3T angefangen, ein dezentrale Typ-3-App technisch zu spezifizieren und diese Überlegungen über Github öffentlich zugänglich zu machen.

Ein Clou der dezentralen Typ-3-App besteht in der Abstandsmessung von Personen per Bluetooth zwischen deren Smartphones durch wechselnde temporäre Kennungen. Wenn Menschen einander zu nahe kommen und zu lange interagieren, besteht ein hohes Infektionsrisiko. Die zweite architektonisch nicht minder bedeutsame Eigenschaft dieses Konzepts besteht darin, dass riskante Begegnungen mit positiv getestet infizierten Personen in der Vergangenheit auf den Smartphones der App-NutzerInnen – nicht auf einem zentralen Server – ermittelt werden. Es obliegt dann den Personen selber, nach einer Warnung durch die App sich in Quarantäne oder Behandlung zu begeben. Der Abgleich von Bluetooth-Kennungen möglicherweise riskanter Kontaktereignisse soll über einen Server geschehen, auch wenn dieser im dezentralen Modell nur eine gemeinsame „Dateiablage" darstellt. Insofern hat die als „dezentral" bezeichnete Architektur mit einem solchen Server – real wären es wohl eine ganze Reihe an geografisch verteilten Servern –

auch ein zentrales Element, nur dass dieser Server außer dem Zwischenspeichern von Daten, die keinen Personenbezug mehr aufweisen, keine weitere Funktion innehat. Insbesondere kann er keine „sozialen Graphen" errechnen wie etwa bei den zentralen Konzepten. Allerdings müssen dafür einige Schutzmaßnahmen angewendet werden, insbesondere bei der Interaktion der Smartphones mit dem zentralen Server. Die AutorInnengruppe war davon überzeugt, dass das Konzept Typ-3 grundsätzlich datenschutzfreundlich funktionieren könnte.

Während der anhaltenden konzeptionellen Arbeiten der AutorInnengruppe am Untersuchungskonzept gab das Robert-Koch-Institut die Wearable-App heraus. Diese App war zwar als *Corona-App* bezeichnet worden, verfolgte aber einen anderen Zweck. Sie sollte der medizinischen Vermessung von Körpern dienen, aber nicht wirkungsvoll Infektionsketten unterbrechen. Das Üble an dieser App ist, dass Menschen hochauflösend ihre Körperfunktionen messen sollen und dann zu einer „Datenspende" ihrer Gesundheitsdaten aufgefordert werden, wobei das RKI die Daten dann nicht direkt vom Smartphone, sondern über die Anbieter der Fitness-Tracker bezieht. Die AutorInnengruppe war in Sorge, dass nun in schneller Folge weitere Apps mit beliebigen, hochzweifelhaften Zwecken auf windigen Rechtsgrundlagen folgen würden.

Die AutorInnengruppe entschied sich daher, das Typ-3-Konzept in Form einer Datenschutz-Folgenabschätzung (DSFA) zu untersuchen, wie sie die Datenschutz-Grundverordnung (DSGVO) in Artikel 35 der verantwortlichen BetreiberIn einer solcher Technik auferlegt. Bei einer DSFA handelt es sich um eine strukturierte Risikoanalyse, die mögliche grundrechtsrelevante Folgen einer Datenverarbeitung im Vorfeld identifiziert. Es werden darin Maßnahmen beschrieben, mit denen diese Risiken adressiert werden oder es wird dargestellt, dass und warum es Schutzmaßnahmen im konkreten Fall nicht gibt oder geben kann. Mit dieser Entscheidung für die Methodik wurden notwendig insbesondere auch die Rechtsgrundlagen für die Nutzung einer Corona-App in den Blick gestellt.

Mit der Entscheidung zur Durchführung einer DSFA zeigte sich umgehend die nächste Schwäche der App des Robert-Koch-Instituts: Wie kann es möglich sein, dass ein Totalmonitoring menschlicher Körperfunktionen zur Praxis wird, ohne dass die Risiken bei der Nutzung dieser App in einer DSFA, so wie es die DSGVO verlangt, offengelegt werden? Eine DSFA durchzuführen ist in jedem Falle obligatorisch, auch (gerade!) wenn Menschen sich freiwillig einer Totalüberwachung aussetzen. Zumal es hieß, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) an der Entwicklung der App beteiligt worden war. Auf Twitter beteuerte der BfDI, dass eine DSFA für diese App vorläge. Diese DSFA wurde bislang nicht veröffentlicht und es wurden keine Aussagen über Prüfmethode und Prüftiefe gemacht.

Die Entscheidung für eine Muster-DSFA nach DSGVO weitete insofern den Blick und generierte unabweisbar einen ganzen Strauß an hochrelevanten Fragestellungen:

- Was genau ist der **Untersuchungsgegenstand**? Aus Datenschutzsicht ist die gesamte Verarbeitungstätigkeit in den Blick zu nehmen, in der eine App und der Betrieb eines zentralen Servers zum Einsatz kommen würden. Die DSGVO verlangt, bei einer Verarbeitungstätigkeit dabei insgesamt mindestens 14 Subprozesse zu unterscheiden, vom Prozess des Erhebens von Daten bis zu deren Löschung (Artikel 4 Absatz 2 DSGVO). Alle Darstellungen zur Corona-App fokussierten bislang technisch auf der Idee mit der Bluetooth-Abstandsmessung, niemand thematisierte bis dahin den anderen, nicht minder schützenswerten Teil des Workflows auf der Serverseite, mit einem Zu-Ende-Denken der gesamten Prozessstruktur, inkl. des Automatisierens von Kommunikationswegen zwischen Ämtern, ÄrztInnen und Betroffenen.

- Welche Instanz ist **verantwortlich für den Betrieb der gesamten Verarbeitungstätigkeit**, inklusive des korrekten Funktionierens der App und der Kommunikationswege? Wer muss entsprechend als datenschutzrechtlich Verantwortliche für die Anfertigung auch der DSFA verantwortlich sein und die Verarbeitung so einrichten, dass sie den Zweck der Infektionskettenunterbrechung – und nichts anderes! – erfüllt und dafür jede Menge an Schutzmaßnahmen installiert werden, bis hin zur Spezifikation, Dokumentation und Offenlegung des Quellkodes, abgeleitet aus dem Transparenzanspruch in Artikel 5 DSGVO.

- Welche **Rechtsgrundlage** muss geschaffen werden und gelten, damit eine solche App tatsächlich rechtskonform eingesetzt werden kann? Wie sind die Betroffenenrechte bzgl. Auskunft oder Korrektur und Widerspruch umgesetzt? Wie muss das System betrieben werden, auch für solche Fälle, in denen fälschlich Daten hochgeladen wurden und diese zurückgerufen werden müssen?

- Wer gilt als **Hauptangreifer** auf die Betroffenen? Es sind nicht die anderen Betroffenen, mit denen in der Vergangenheit Kontakt bestand. Aus Datenschutzsicht ist der Hauptangreifer des Verfahrens immer derjenige, der das Verfahren betreibt, denn dieser ist maximal mächtig und in der Regel auch daran interessiert, um über den Zweck hinaus weitere Daten zu erheben oder diese Daten auch noch für andere Zwecke zu verarbeiten. Und wenn er nachlässig die Daten verarbeiten (lässt), dann können wiederum Unbefugte Zugriff auf diese Daten nehmen. Und weiterhin besteht grundsätzlich für jede App-Konzeption das Problem, wie Betroffene vor den Aktivitäten von Apple und Google zu schützen sind, die das Betriebssystem stellen, mit dem einerseits die Bluetooth-Signale und temporären Kennungen (tempIDs) erzeugt werden und die die Schnittstelle zur App bilden? Die App steuert die gesamte Technik inklusive des Uploads und Downloads von tempIDs. Apple und Google sind technisch in der Lage, aber nicht befugt, Zugriff auf die tempIDs zu nehmen. In der DSFA wird ein Angriff untersucht, der zeigt, wie in diesem Verfahren die Daten auch unbeteiligter Android-NutzerInnen gespeichert werden.

- Welche **Modellierung der Risiken** wird gewählt? Die Risikomodellierung aus Datenschutzsicht besteht darin, dass die Verarbeitung nicht (hinreichend) die Grundsätze des Artikel 5 DSGVO erfüllt. Eine Risikomodellierung nimmt diese Grundsätze auf und entwickelt an diesen entlang eine Heuristik. Und weil Datenschutz permanent sicherzustellen ist, muss seitens der Verantwortlichen ein Datenschutz-

Management betrieben werden, mit dem kontinuierlich Störungen und Fehlfunktionen entdeckt, geprüft und wirksam behoben werden.

- Welche **Angriffe** zum vorsätzlichen Unterlaufen des Systems oder zur (Zer-) Störung der Funktionalität sind denkbar und wahrscheinlich?

- Mit welchen **Schutzmaßnahmen** lassen sich die identifizierten Risiken so verringern, dass die Anforderungen der DSGVO hinreichend erfüllt sind und ein verantwortbarer, beherrschbarer Betrieb des Verfahrens aufgenommen werden kann? Denn das Ergebnis einer DSFA besteht in einem **DSFA-Bericht** an die Verantwortliche, die diese Empfehlungen bzgl. der Gestaltung des Verfahrens und des kontrollierten Betriebs von Schutzmaßnahmen, etwa zur Pseudonymisierung oder zur Anonymisierung von Daten, dann umsetzen und deren Wirksamkeit gem. Art. 35 nachweisen muss. Wenn der Betrieb trotz Schutzmaßnahmen weiterhin zu hohe Risiken birgt beziehungsweise ein zu geringes Schutzniveau für die Betroffenen aufweist, kann die Verantwortliche Kontakt zur zuständigen Datenschutz-Aufsichtsbehörde nehmen und dort um eine Empfehlung bitten. Dabei kann sich herausstellen, dass eine geplante Datenverarbeitung grundsätzlich nicht betrieben werden kann.

Sowohl bei der Bestimmung und Modellierung der Risiken in Bezug auf die erzeugten Daten, die beteiligten IT-Systeme und die Prozesse als auch beim Bestimmen wirksamer Schutzmaßnahmen griff die AutorInnengruppe auf das Standard-Datenschutzmodell-V2a (SDM) zurück. Neben dem SDM, das die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) seit 2018 zur Nutzung empfehlen, wurden unter anderen insbesondere das DSK-Kurzpapier Nr. 5 zur systematischen Durchführung der DSFA und das Working Paper Nr. 248 der Artikel-29-Arbeitsgruppe zur Analyse der Risikohöhe diese Verfahrens („Schwellwert-Analyse“) herangezogen.

Auf diese Weise strebte die AutorInnengruppe an, in möglichst vorbildlicher Weise sowohl den technischen, als auch den rechtlichen und methodischen Maßstab dafür auszuweisen, wie die Funktionen und die daraus sich ergebenden Datenschutz-Risiken einer Tracing-App für Betroffene in Zukunft zu analysieren, zu bestimmen und gegebenenfalls zu verringern sind.

Eine DSFA nach Artikel 35 DSGVO hat allerdings zwei Schwächen. Sie ist keine wissenschaftliche Technikfolgenabschätzung. Das bedeutet, dass sie von der Verantwortlichen weder eine gesellschaftliche Kontextierung der geplanten Verarbeitung noch eine Veröffentlichung der DSFA verlangt. Die AutorInnengruppe ist jedoch der Ansicht, dass ein Contact-Tracing-Verfahren mit einem derart hohen Risiko für die Grundrechte und mit der enormen Tragweite der Akzeptanz einer Überwachungs-App für die Gesellschaft insgesamt, grundsätzlich in den gesellschaftlichen Kontext gestellt werden sollte. Eine Überwachungs-App und überhaupt alle derartig eingriffsintensiven Systeme müssen mit ihren Risiken und deren Bearbeitung durch die verantwortliche Organisation einem öffentlichen Diskurs unterstehen, weswegen die dazugehörigen DSFAen grundsätzlich veröffentlicht werden sollten.

Referenz

Datenschutz-Folgenabschätzung (DSFA) für die Corona-App,
https://www.fiff.de/presse/dsfa-corona

FIfF e. V.

Empfehlungen für die Verantwortlichen

zur Gestaltung der Verarbeitung und Umsetzung der identifizierten Schutzmaßnahmen

Diese DSFA-Projektgruppe empfiehlt der Verantwortlichen für das Verfahren, mit dem riskante Kontakte mit COVID-19-infizierten Personen unter Zurhilfenahme einer Smartphone-App identifiziert werden sollen, die Gestaltung der Verarbeitung und das Treffen von Schutzmaßnahmen wie folgt anzugehen, um die Anforderungen der DSGVO umzusetzen:

1. Es müssen geeignete Rechtsgrundlagen geschaffen und Verantwortlichkeiten geklärt werden. Die Verarbeitung als „freiwillig“ auszuweisen und auf der Grundlage von Einwilligungen umzusetzen, genügt den datenschutzrechtlichen Anforderungen nicht, insbesondere weil Zweifel an der Freiwilligkeit und Informiertheit bestehen. Stattdessen müssen gesetzliche Grundlagen geschaffen werden, die diese Anforderungen, insbesondere zur Zweckbindung, zur Anonymisierung, zum Löschkonzept und zum Datenschutzmanagement, umsetzen. Dabei ist nicht allein auf die technischen Spezifikationen einer App zu achten, sondern es ist das gesamte Verfahren einschließlich der Schnittstellen, zum Beispiel Einbindung in das geplante elektronische Meldeverfahren, zu berücksichtigen. Ebenso sind unerwünschte technische und soziale Nebenwirkungen, die Einfluss auf die Grundrechtsausübung nehmen und sich damit auch mittelbar auf die Akzeptanz des Verfahrens auswirken, zu berücksichtigen. So muss sichergestellt werden, dass Dritte keine Einsicht in die App und ihre Anzeigen auf den Smartphones von Betroffenen nehmen können. Die GesetzgeberIn muss eine Verordnung nach § 14 Absatz 8 IfSG erlassen, die technische Anforderungen datenschutzkonform konkretisiert.

2. An zwei Stellen der gesamten Prozesskette ist der Personenbezug besonders heikel; nämlich im Kontext der Erstellung und Speicherung der TempIDs sowie im Kontext des Uploads der Gesundheits-TempIDs von CV-infizierten Personen und ihrer Speicherung auf dem Server. Diese neuralgischen Stellen müssen wie folgt gestaltet werden:

a. Bei der Erstellung der TempIDs in der App muss sichergestellt werden, dass es keine Verkettung zwischen TempIDs gibt und geben kann. Eine konkrete TempID darf also nicht aus der zeitlich vorhergehenden oder anderen gemeinsamen Komponenten abgeleitet werden können. Die TempIDs müssen in der App so gespeichert werden, dass sich nachträglich nicht feststellen lässt, in welcher Reihenfolge sie erzeugt und gespeichert wurden.

b. Die BetreiberIn des oder der Server muss ein wirksames Trennungsverfahren einsetzen, das Gesundheits-TempIDs aus den Apps von COVID-19-infizierten Personen auf dem Server in Infektionsanzeigende Daten ohne Personenbezug (iDoP) transformiert und das rechtlich, organisatorisch und technisch abgesichert geschieht (Podlech 1976). Rechtlich muss die BetreiberIn eine unabhängige Stelle sein, die keine eigenen Interessen an den Daten haben darf und vor Pflichten zur Herausgabe von Daten geschützt ist, auch gegenüber Sicherheitsbehörden. Organisatorisch müssen die Verantwortliche strategisch und die BetreiberIn operativ eine Mixstruktur etablieren, die dafür sorgt, die funktionale Differenzierung bzw. die informationelle Gewaltenteilung innerhalb der Organisation durchzusetzen – so, wie beispielsweise Rechtsprechung und Gerichtsverwaltung zusammen und doch getrennt in der Gerichtsorganisation arbeiten. Die BetreiberIn muss ein Datenschutzmanagement etablieren, das es erlaubt, die Trennung prüfbar wirksam durchzusetzen und aufrechtzuerhalten. Technisch muss sie die Trennung so umsetzen, dass Uploads der Gesundheits-TempID nicht protokolliert werden können, weder auf dem Server noch im Netzwerk der BetreiberIn. Darüber hinaus muss der Upload der Gesundheits-TempIDs zwischen Apps und Servern Ende-zu-Ende-verschlüsselt erfolgen und durch die Nutzung vorgeschalteter Anonymisierungsproxies (z. B. Tor) gesichert werden. Im Rahmen einer Datenschutzkontrolle muss das Trennungsverfahren einer stetigen Prüfung durch die zuständige Datenschutzaufsichtsbehörde unterliegen.

Die IT-Sicherheit der genutzten IT-Komponenten in der gesamten Prozesskette, unter Einbeziehung auch der Interaktion mit ÄrztInnen und Gesundheitsämtern, muss nach BSI IT-Grundschutz oder im Rahmen von ISO-27001 zertifiziert werden. Hier sind insbesondere Aspekte der Sicherstellung der Verfügbarkeit, insbesondere der Server (-Infrastrukturen), der Authentisierung der beteiligten IT-Komponenten sowie der Vertraulichkeit der Kommunikationsbeziehungen für hohen Schutzbedarf zu beachten.

3. Flankierend zur Veröffentlichung der App muss rechtlich und faktisch sichergestellt werden, dass NutzerInnen Dritten gegenüber weder den Status der App noch die Existenz der App auf dem eigenen Gerät bekannt geben müssen. Eine Ausnahme könnte ärztliches Personal bilden, um Heimquarantäne auch bei ArbeitgeberInnen anhand von Krankschreibungen durchzusetzen. Ziel dieser Regelungen ist das Sicherstellen der Zweckbindung der Aktivitäten der App. Zugangskontrollen zu öffentlichen und privaten Gebäuden, Universitäten, Schulen, Transportmitteln, Verwaltungen, Polizeidienststellen etc., bei denen eine Einsichtnahme in die App verlangt wird, sind zu unterbinden.

4. Vor Veröffentlichung der App muss von einer unabhängigen Stelle eine umfassende Software- und Gesamtsystem-Untersuchung durchgeführt und veröffentlicht werden. Hierbei ist insbesondere auch auf die Risiken zu achten, die sich aus Interaktionen mit Betriebssystem-Komponenten ergeben und potenziell auch für Nicht-NutzerInnen der App relevant sind (siehe Angriffsszenario B5 in Kapitel 7). An der Kooperationsbereitschaft großer Plattformunternehmen (Google, Apple) oder an rechtlichen bzw. faktischen Hürden bei der Sicherstellung von Datenschutzvorgaben (siehe etwa den US-CLOUD-Act oder das PRISM-Programm der National Security Agency) könnte dieser Punkt scheitern. Sollte etwa das Risiko nicht ausgeschlossen werden können, dass Plattformen die Kontaktereignisse mitlesen und das Matching mit infizierten Personen selbst durchführen können, wäre die Einstellung des Vorhabens einer Corona-App die gebotene Konsequenz.

Das FIfF bittet um Eure Unterstützung

Viermal im Jahr geben wir die FIfF-Kommunikation heraus. Sie entsteht durch viel ehrenamtliche, unbezahlte Arbeit. Doch ihre Herstellung kostet auch Geld – Geld, das wir nur durch Eure Mitgliedsbeiträge und Spenden aufbringen können.

Auch unsere weitere politische Arbeit kostet Geld für Öffentlichkeitsarbeit, Aktionen und Organisation. Unsere jährlich stattfindende FIfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen, Kommunikation im Web: Neben der tatkräftigen Mitwirkung engagierter Menschen sind wir bei unserer Arbeit auf finanzielle Unterstützung angewiesen.

Bitte unterstützt das FIfF mit einer Spende. So können wir die öffentliche Wahrnehmung für die Themen weiter verstärken, die Euch und uns wichtig sind.

Spendenkonto:
Bank für Sozialwirtschaft (BFS) Köln
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

EDRi calls for fundamental rights-based responses to COVID-19

The Coronavirus (COVID-19) disease poses a global public health challenge of unprecedented proportions. In order to tackle it, countries around the world need to engage in co-ordinated, evidence-based responses. Our responses should be grounded in solidarity, support and respect for human rights, as the Council of Europe Commissioner for Human Rights has highlighted.[1] The use of high-quality data can support the vital work of scientists, researchers, and public health authorities in tracking and understanding current pandemic.

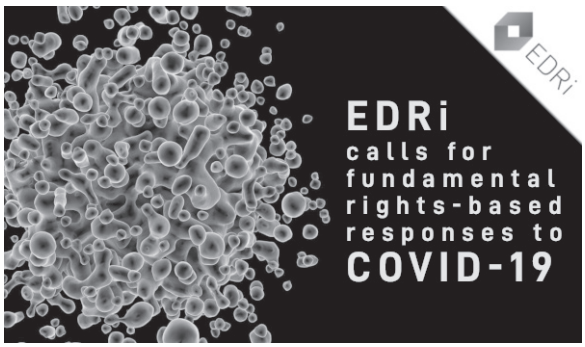
However, some of the actions taken by governments and businesses under exceptional circumstances today, can have significant repercussions on freedom of expression, privacy and other human rights both today and tomorrow. We are already seeing the launch of legal initiatives to tackle misinformation[2], but sometimes with disproportionate reactions[3] from governments. Similarly, we are witnessing a surge in emergency-related policy initiatives[4], some of them risking the abuse of sensitive personal data in an attempt to safeguard public health[5]. When acting to address such a crisis, measures cannot lead to disproportionate and unnecessary actions, and it is also vital that measures are not extended once we are no longer in a state of emergency.

In these circumstances, European Digital Rights (EDRi) calls on the Member States and institutions of the European Union (EU) to ensure that, while taking public health measures to tackle COVID-19, they:

- **Strictly uphold fundamental rights:** Under the European Convention on Human Rights, any emergency measures which may infringe on rights must be[6] "temporary, limited and supervised" in line with the Convention's Article 15, and cannot be contradictory to international human rights obligations. Similar wording can be found in Article 52.1 of the EU Charter of Fundamental Rights. Actions to tackle coronavirus using personal health data, geolocation data or other metadata must still be necessary, proportionate and legitimate, must have proper safeguards[7], and cannot excessively undermine the fundamental right to a private life.

- **Protect data for now and the future:** Under the General Data Protection Regulation (GDPR) and the E-Privacy Directive, location data is personal data, and therefore is subject to high levels of protection even when processed by public authorities or private companies. Location data revealing movement patterns of individuals is notoriously difficult to anonymise, although many companies claim that they can do this. Data must be anonymised to the fullest extent, for example through aggregation and statistical counting. COVID-19 cannot be an opportunity for private entities to profit, but rather can be an opportunity for the EU's Member States to adhere to the highest standards of data quality, processing and protection, with the guidance of national data protection authorities, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).

- **Limit the purpose of data for COVID-19 crisis only:** Under law, the data collected, stored and analysed in support of public health measures must not be retained or used outside the purpose of controlling the coronavirus situation.



- **Implement exceptional measures only for the duration of the crisis:** The necessity and proportionality of exceptional measures taken during the COVID-19 crisis must be reassessed once the crisis is ameliorated. Measures should be time limited and subject to automatic review for renewal at short intervals.

- **Keep tools open:** To preserve public trust, all technical measures to manage coronavirus must be transparent and must remain under public control. In practice, this means using free/open source software when designing public interest applications.

- **Condemn racism and discrimination:** Measures taken should not lead to discrimination of any form, and governments must remain vigilant to the disproportionate harms that marginalised groups can face.

- **Defend freedom of expression and information:** In order to take sensible, well-informed decisions, we need access to good-quality, trustworthy information. This means protecting the voices of human rights defenders, independent media, and health professionals more than ever. In addition to this, the increased use of automated tools to moderate content[8] as a result of fewer human moderators being available needs to be carefully monitored. Moreover, a complete suspension of attention-driven advertising and recommendation algorithms should be considered to mitigate the spread of disinformation that is already ongoing.

- **Take a stand against internet shutdowns:** During this crisis and beyond, an accessible, secure, and open internet will play a significant role in keeping us safe[9]. Access for individuals, researchers, organisations and governments to accurate, reliable and correct information will save lives. Attempts by governments to cut or restrict access to the internet, block social media platforms or other communications services, or slow down internet speed will deny people vital access to accurate information, just when it is of paramount

importance that we stop the spread of the virus. The EU and its Member States should call on governments to immediately end any and all deliberate interference with the right to access and share information, a human right and vital to any public health and humanitarian response to COVID-19.

- **Companies should not exploit this crisis for their own benefit:** Tech companies, and the private sector more broadly, need to respect existing legislation in their efforts to contribute to the management of this crisis. While innovation will hopefully have a role in mitigating the pandemic, companies should not abuse the extraordinary circumstances to monetise information at their disposal.

Referenzen

Coronavirus: New ARTICLE 19 briefing on tackling misinformation (16.03.2020) https://www.article19.org/resources/coronavirus-new-article-19-briefing-on-tackling-misinformation/

EFF: Protecting Civil Liberties During a Public Health Crisis (10.03.2020) https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis

People First: Wikimedia's Response to COVID-19 (15.03.2020) https://medium.com/freely-sharing-the-sum-of-all-knowledge/wikimedia-coronavirus-response-people-first-8bd99ea6214b

Access Now: Protect digital rights, promote public health: toward a better coronavirus response (05.03.2020) https://www.accessnow.org/protect-digital-rights-promote-public-health-towards-a-better-coronavirus-response/

Privacy International – Tracking the Global Response to COVID-19 (19.03.2020) https://privacyinternational.org/examples/tracking-global-response-covid-19

noyb: Data Protection under COVID-19 https://gdprhub.eu/index.php?title=Data_Protection_under_COVID-19

Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak (16.03.2020) https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

Anmerkungen

1 *https://www.coe.int/en/web/commissioner/-/we-must-respect-human-rights-and-stand-united-against-the-coronavirus-pandemic*
2 *https://www.article19.org/resources/coronavirus-new-article-19-briefing-on-tackling-misinformation/*
3 *https://activewatch.ro/ro/freeex/reactie-rapida/prin-lipsa-de-transparenta-institutiile-statului-alimenteaza-conspirationismul-si-dezinformarea/*
4 *https://privacyinternational.org/examples/tracking-global-response-covid-19*
5 *https://twitter.com/gemmagaldon/status/1240364204818866176*
6 *https://www.echr.coe.int/Documents/FS_Derogation_ENG.pdf*
7 *https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en*
8 *https://www.bbc.com/news/technology-51926564*
9 *https://www.accessnow.org/keepiton-internet-shutdowns-during-covid-19-will-help-spread-the-virus/*

Humanistische Union

Grundrechte gehören nicht in Quarantäne

Die Humanistische Union formuliert Forderungen zur Corona-Pandemie

Die Humanistische Union versteht sich als radikale Verfechterin der Grund-, Bürger- und Menschenrechte in ihrer ganzen Breite. Sie sieht heute mit Sorge, wie diese Rechte in der momentanen Krisensituation zunehmend eingeschränkt werden. Von den einschränkenden Maßnahmen sind nahezu alle Grundrechte betroffen. Grundrechte sind aber keine Schönwetterrechte, sie sollen sich gerade auch in Bedrohungslagen bewähren! Sie müssen daher gerade in Zeiten wie diesen, wo ihre weitgehende Aussetzung von einer Mehrheit unterstützt wird, verteidigt werden. „Das Corona-Virus hat unser Leben in einem vorher unvorstellbarem Maße in eine Zwangspause katapultiert, aber für die Verteidigung von Grundrechten gibt es keine Pause", erklärte Werner Koep-Kerstin, der Bundesvorsitzende der Humanistischen Union.

Nur wenn jeder Grundrechtseinschränkung transparente und demokratische politische Entscheidungen zugrunde liegen, kann die notwendige Akzeptanz einschneidender Maßnahmen weiter gewährleistet werden. Der fast vollständige Übergang der Entscheidungsgewalt an die Exekutive des Staates in Bund und Ländern ohne parlamentarische Mitwirkung ist erschreckend. Die zur Bekämpfung der Pandemie getroffenen Maßnahmen resultieren in einer Form von Ausnahmezustand, wie es ihn seit dem Zweiten Weltkrieg nicht mehr gegeben hat. Es ist unerlässlich, dass ausschließlich demokratische Institutionen über derartige Maßnahmen entscheiden – und nur im Rahmen der ihnen vom Grundgesetz verliehenen Kompetenzen. Das gilt sowohl für die klassischen drei Gewalten als auch für die föderalen Strukturen. Politische Entscheidungen müssen transparent vorbereitet und getroffen werden; wissenschaftliche Erkenntnisse sind dafür die Grundlage, dürfen aber die Entscheidungen nicht determinieren. Es gibt keine *alternativlosen* Entscheidungen!

Die Humanistische Union fordert:

- Jede Maßnahme, die wegen der Pandemie Grundrechte einschränkt oder ihre Geltung aussetzt, muss befristet sein. Bevor die Fortgeltung solcher Maßnahmen angeordnet wird, muss demokratisch überprüft werden, ob sie zur Erreichung des angestrebten Ziels noch die geeignetsten und mildesten Mittel sind, und ob sie noch angemessen sind. Dazu gehört die transparente und sorgfältige Abwägung der mit der Grundrechtseinschränkung verbundenen Risiken. Bei allen Maßnahmen müssen auch die damit verbundenen anderen Risiken (z. B. das Risiko häuslicher Gewalt) berücksichtigt werden.

- Zu einer demokratischen Überprüfung der Fortgeltung von Grundrechtseinschränkungen gehört zwingend die Mitwirkung parlamentarischer Körperschaften. Anderslautende Ermächtigungen der Exekutive sind wegen ihrer Verfassungswidrigkeit aufzuheben.

- Einschränkungen des Versammlungsrechts, die über das durch den Infektionsschutz gebotene Maß hinausgehen, sind sofort zurückzunehmen. Die Humanistische Union begrüßt daher die jüngste Entscheidung des Bundesverfassungsgerichts, dass bei Anmeldungen von Versammlungen die Behörden ihren Ermessensspielraum nutzen und konkrete Einzelfallprüfungen vornehmen müssen.

- Derzeit wird über eine *Corona-App* als Allheilmittel zur Nachverfolgung von Infektionsketten zur Eindämmung der Pandemie diskutiert. Der stellvertretende Bundesvorsitzende der Humanistischen Union, der Informatiker Stefan Hügel, warnt: *„Eine solche Corona-App birgt erhebliche Risiken für den Datenschutz und damit für die Persönlichkeitsrechte bei gleichzeitig unklarem Nutzen für den angestrebten Zweck." Die Erwartungen an* eine *Corona-App* müssen daher klar formuliert werden, und die App muss so entwickelt werden, dass sie ihren Zweck und die notwendigen Datenschutzstandards erfüllt.

- Es müssen datenschutzfreundliche und sichere Lösungen für mobiles Arbeiten entwickelt werden. Dabei müssen die Lasten gerecht und nicht einseitig auf die Arbeitnehmer abgewälzt werden.

- Die staatlichen Versäumnisse bei der Digitalisierung müssen aus aktuellem Anlass benannt werden, um sie zu beseitigen.

- Die Privatisierung großer Teile der öffentlichen Infrastruktur muss auf den Prüfstand.

- Es muss im Hinblick auf zukünftige Krisen, insbesondere in Folge des Klimawandels, geklärt werden, was wir aus der Corona-Krise lernen können bzw. müssen. Die Wahrung der Grundrechte muss Staat und Gesellschaft bei jeder Krisenbewältigung leiten.

- Die Notversorgung und Evakuierung der Flüchtlinge in den durch die Corona-Krise besonders bedrohten Flüchtlingslagern an der Südgrenze der Europäischen Union müssen durch eine europäische, humanitäre Lösung sichergestellt werden.

Diese Pressemitteilung beruht auf einem Positionspapier der Humanistischen Union zur Corona-Krise. Das Papier kann auf der Webseite der Humanistischen Union (www.humanistische-union.de) abgerufen werden.

Die Zivilgesellschaft

Aus der Krise lernen: Digitale Zivilgesellschaft stärken!

Als zivilgesellschaftliche Organisationen, die sich für eine unabhängige digitale Infrastruktur und freien Zugang zu Wissen einsetzen, fordern wir: „Der Aufbau eines gemeinwohlorientierten digitalen Ökosystems muss endlich politische Priorität bekommen!"

In Krisensituationen zeigt sich die Bedeutung von unabhängigen und belastbaren digitalen Infrastrukturen, die es Menschen, Organisationen und Firmen ermöglichen, ihren alltäglichen Aufgaben nachzukommen. Von den Umstellungen zur Eindämmung von Covid-19 haben bislang vor allem die großen Technologiekonzerne profitiert: Die Verlagerung des Lebens in die digitale Sphäre beschert ihnen größere Marktanteile, Nutzungszahlen und Datensammlungen. Um in Krisenzeiten nicht von ihnen abhängig zu sein, braucht es ein aktives digitales Ökosystem, das echte Wahlmöglichkeiten bietet.

Software und dezentrale Plattformen ohne kommerziellen Hintergrund stammen oft aus gemeinwohlorientiertem Engagement. Nicht nur Unternehmen und Selbständigen bricht gerade die Finanzierung weg, sondern auch ehrenamtlich getragenen Organisationen. Wichtige Teile unserer digitalen Infrastruktur beruhen auf ihrer Arbeit. Für sie gibt es aber kein milliardenschweres Hilfspaket.

Um besser vorbereitet zu sein für zukünftige Krisensituationen, muss ihre Arbeit gestärkt werden. Das Gute ist: Es gibt bereits ein weitreichendes Netz an Menschen und Organisationen, die gemeinsam an dezentraler und damit widerstandsfähiger digitaler Infrastruktur arbeiten und so die Grundlage dafür schaffen, dass wir in der nächsten Krise besser aufgestellt sind. Sie arbeiten an freiem Zugang zum Internet wie die Initiativen für freie Funknetze, der Bereitstellung von sicheren Kommunikationswegen, Angeboten zu Freiem Wissen bis hin zu Open-Data- und Freien-Software-Anwendungen. Bisher erhalten sie dafür noch nicht genug Unterstützung von öffentlicher Seite. Jetzt liegt es an der Politik, auf sie zuzugehen und sie zu unterstützen.

Um langfristig und damit nachhaltig zivilgesellschaftliches Engagement und den Erhalt eines gemeinwohlorientierten digitalen Ökosystems zu fördern, schlagen wir folgende konkrete Maßnahmen vor – denn nach der Krise ist vor der Krise, wenn alles beim Alten bleibt:

Öffnung der Digitalpolitik für gesellschaftlichen Input

Digitalpolitik, die das Gemeinwohl ins Zentrum stellt, lässt sich nur gemeinsam mit gesellschaftlichen Akteurinnen, Akteuren und Initiativen verwirklichen. Hierfür muss sich die Politik noch weiter für Vorschläge aus der Gesellschaft öffnen und diese in die Politikgestaltung miteinbeziehen. Dazu braucht es die Anerkennung zivilgesellschaftlicher Expertise und ein klares Bekenntnis, deren Wissen und Kompetenzen zu nutzen.

Gezielte Förderung

Die digitale Zivilgesellschaft ist nur durch das ehrenamtliche Engagement und die Spenden von Bürgerinnen und Bürgern arbeitsfähig. Gerade in Krisensituationen brechen diese Stützpfeiler schnell weg und bedrohen die Existenz von Vereinen, Stiftungen und Initiativen.

In Deutschland mangelt es an niedrigschwelliger finanzieller Unterstützung für Organisationen und Sozialunternehmen aus der digitalen Zivilgesellschaft. Es braucht neue Fördermechanismen, die den Aufbau nachhaltiger Strukturen unterstützen und nicht nur Innovation im Blick haben, sondern auch die Instandhaltung und Weiterentwicklung bestehender Technologien. Möglich wäre eine solche Förderung beispielsweise durch eine vom Bund geförderte Stiftung öffentlichen Rechts, die Entwicklung, Wartung und Bereitstellung digitaler Technologien für die Gesellschaft fördert.

Öffentliches Geld, Öffentliches Gut

Es braucht rechtliche Grundlagen, die es verpflichtend machen, dass mit öffentlichen Geldern erarbeitete Inhalte offen zugänglich und weiterverwendbar gemacht werden. Der Datenschutz muss dabei immer gewahrt sein.

Dazu gehören: öffentlich finanzierte Software, Datenbestände und Informationen öffentlicher Stellen, Forschungs- und Bildungsinhalte öffentlich getragener Institutionen sowie die Inhalte des öffentlich-rechtlichen Rundfunks.

Entwicklung öffentlicher digitaler Infrastruktur

Wir empfehlen kontinuierliche staatliche Investitionen in die Entwicklung und Instandhaltung digitaler Infrastruktur und den Aufbau widerstandsfähiger Netze.

Wir fordern die Förderung von Dezentralisierung und einem breiten Ökosystem von Betreibern digitaler Infrastruktur, um digitale Souveränität zu erlangen und Abhängigkeiten von einzelnen Anbietern aufzulösen, durch den Abbau von Betreibermonopolen sowie dem konsequenten Einsatz von offenen Standards, Freier- und Open-Source-Software-Technologien.

Unterzeichnende Organisationen:

Free Software Foundation Europe (fsfe), Digitale Gesellschaft, epicenter.works – for digital rights, Chaos Computer Club, Wikimedia Deutschland, Superrr Lab, D64 – Zentrum für digitalen Fortschritt, Stiftung neue Verantwortung, Prototype Fund, iRights.lab – Think Tank für die digitale Welt, Algorithmwatch, Nextcloud, FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Open Knowledge Foundation Deutschland, Bundesverband deutscher Stiftungen, gig – Global Innovation Gathering, freifunk.net, Ashoka, Center for the Cultivation of Technology, Bits & Bäume – Digitalisierung und Nachhaltigkeit, Simply Secure, SEND – Social Entrepreneurship Netzwerk Deutschland, Stiftung Erneuerbare Freiheit, Verstehbahnhof, Goethe-Institut, OpenData.ch, Retune, Digitale Freiheit, BIB – Bundesverband Information Bibliothek, linuxmuster.net, Akademie für Ehrenamtlichkeit Deutschland, AStA TU Berlin, Bits & Bäume Berlin, #DMW – Digital Media Women, Public Beta, Privacy Week Berlin, NODE – Forum for Digital Rights, BildungsCent, Landesbibliothekszentrum Rheinland-Pfalz, Deutscher Bundesjugendring, youvo, IfZ – Initiative für Zukunftsverantwortung, Open Government Netzwerk Deutschland, Citizens for Europe, Nitrokey – secure your digital life, Seitenstark, Liquid Democracy, European Hub for Civic Engagement, BUNDjugend – Young Friends of the Earth, Selbstbestimmt.digital, FFII – Förderverein für eine freie Informations-Infrastruktur, Germanwatch, Digital Guerilla, freie.it, Education Innovation Lab, heldenrat – Beratung für soziale Bewegungen, cbm. Computer Bildung Medien, Das progressive Zentrum, Civil Liberties Union for Europe, Rosy DX, www.aufdraht.org, The Urban Tech Republic Berlin TXL, Phineo – damit Engagement wirkt, Computertruhe, FOSSGIS, Social Impact, Stiftung Ecken wecken, Wechange, Stiftung Bürgermut, Project Together, et – Evangelische Trägergruppe für gesellschaftspolitische Jugendbildung, dbv – Deutscher Bibliotheks-Verband, hackerfleet, The Isomer Community, betterplace.lab, Evangelische Schule Berlin Zentrum, ownCloud, ifa – Institut für Auslandsbeziehungen, GGC – Global Goals Curriculum 2030, In-Haus

FIfF e. V.

Grundrechtseinschränkungen in Zeiten von Corona

über Verhältnismäßigkeit, Technikeinsatz und überzogene Erwartungen

12. April 2020 – *Aktuell wird viel über die Einschränkung von Grundrechten zum Schutze der Bevölkerung diskutiert, dabei geht es um Themen wie Ausgangsbeschränkungen oder das Auswerten von Bewegungs- oder Kontaktdaten, beides zum scheinbar übergeordneten Zweck der Pandemieeindämmung. Gerade bei zweiterem fallen dann Sätze wie „Datenschutz kostet Leben", was beängstigend an das ebenso falsche „Datenschutz ist Täterschutz" erinnert. Dabei müsste in diesen Diskursen eigentlich klar sein, dass es hier keine eindeutig gebotenen Handlungen gibt. Es stehen sich unvereinbare Grundrechte gegenüber, so dass die Stärkung einer Seite immer zulasten der anderen geht. So mag eine Ausgangsbeschränkung das Recht auf Leben und körperliche Unversehrtheit schützen, sie schränkt jedoch im gleichen Atemzug die Bewegungsfreiheit, Freizügigkeit und sogar Demonstrationsfreiheit ein. Gleiches gilt für die Nutzung von Bewegungsdaten aus dem Mobilfunknetz oder anderer Ortsdaten zur Verfolgung von Infektionsketten. Diese greift ganz wesentlich in das Grundrecht auf Datenschutz und sogar die Menschenwürde ein.*

Tatsächlich müssen in diesen und anderen Fällen also verschiedene gegenläufige Grundrechte gegeneinander abgewogen werden. Das muss immer in Bezug auf ganz konkrete Maßnahmen und ihre konkrete Ausgestaltung passieren. Bevor eine letzliche politische Entscheidung getroffen werden kann, braucht es während der Abwägungsphase natürlich auch verschiedene fachliche Kompetenzen, um die Implikationen und Handlungsspielräume zu erörtern. Darum äußert sich das FIfF zu den aktuellen technischen Fragestellungen, denn hier kommt es auf das technische Detail und die konkrete Ausgestaltung an.

Das Verhältnismäßigkeitsprinzip

Zunächst jedoch ein paar Worte zum üblichen methodischen Vorgehen dieses Abwägungsvorgangs. Die verfassungstheoretische Grundlage ist dabei das sogenannte Verhältnismäßigkeitsprinzip. Dabei wird eine grundrechteeinschränkende Maßnahme in vier grundsätzlichen Schritten analysiert. Diese fragen konkret danach, ob die Maßnahme

- einem legitimen Zweck dient,
- geeignet ist, diesen Zweck zu erreichen,
- erforderlich ist, diesen Zweck zu erreichen (es also kein milderes, gleich geeignetes Mittel gibt) und
- ob die Maßnahme angemessen ist.

Eine Maßnahme ist dann legitim, wenn ihr Zweck grundsätzlich im Bereich der dem Staate übertragenen Aufgaben liegt. Geeignet ist sie, wenn sie diesem Zweck grundsätzlich kausal dienen kann. Erforderlich ist sie, wenn kein schwächeres Mittel geeignet ist, diesem Zweck zu dienen. Angemessen – oder verhältnismäßig im engeren Sinne – ist eine Maßnahme, wenn die Schwere der Grundrechtseingriffe bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Im letzten Schritt findet also eine sogenannte Rechtsgüterabwägung statt. Diese ist niemals nur rechtlich abhandelbar, sondern hat immer auch eine politische Dimension.

Beispiel: Corona-App

Wenden wir dieses Schema nun beispielhaft auf ein aktuelles Anwendungsszenario mit Technikbezug an, eine *Corona-App*.

Legitimer Zweck

Der übergeordnete Zweck der Corona-App ist in der Regel jedenfalls mittelbar angesiedelt beim Schutz des Lebens und der körperlichen Unversehrtheit von Personen während einer Pandemie; sie dient also insgesamt gesehen der Pandemieeindämmung und -steuerung, konkret derzeit der Verzögerung von Neuansteckungen, um das Gesundheitswesen nicht über seine Leistungsfähigkeit zu belasten. Dieses Ziel können Individuen nicht allein verfolgen, daher ist es ein legitimer Zweck für staatliche Stellen. Konkrete Maßnahmen brauchen jedoch einen konkreten Zweck, erst dann kann auch über eventuellen Technikeinsatz nachgedacht werden. Beispielhaft betrachten wir an dieser Stelle zwei Szenarien:

Zweck A sei die Informierung potenziell Infizierter, also die Warnung an Menschen, die mit Infizierten Kontakt hatten, sodass diese sich in Quarantäne begeben können.

Zweck B sei an dieser Stelle die allgemeine Überprüfung der Einhaltung von Ausgangsbeschränkungen, um politisches Handeln zu evaluieren.

Die Beispielzwecke können dabei durch den Einsatz jeweils verschiedener Technik verfolgt werden oder aber ganz ohne. Die Zweckfrage an sich ist allerdings keine technische Frage.

Geeignetheit

Dieser Aspekt hat jedoch eine technische Dimension, denn wenn eine bestimmte Technologie dem Zweck gar nicht dienen kann, so darf sie auch nicht eingesetzt werden.

Zweck A: Da eine technische Evaluation von GPS- oder Mobilfunk-Metadaten ergibt, dass diese Daten für die Feststellung epidemiologisch relevanter Kontaktereignisse nicht genau genug sind, scheiden diese Technologien aus. Nahbereichstechnologien wie etwa Bluetooth hingegen sind geeignet, weil sie u. a. sogar für Entfernungsmessungen im Meterbereich gedacht sind.

Zweck B: Zur Erstellung allgemeiner Bewegungsstatistiken einer Bevölkerung, so wie sie für Beispiel B benötigt werden, wären GPS- oder Mobilfunk-Metadaten technisch geeignet. Die Nahbereichstechnologien wiederum sind nur bedingt geeignet, weil sie nicht ohne weiteres einen Ortsbezug aufweisen. Ebenfalls geeignet wären aggregierte Daten, also zusammengefasste und rein statistische Daten, die aus GPS-, Mobilfunkmeta- oder Nahbereichsdaten errechnet werden können.

Erforderlichkeit

Dieser Aspekt hat ebenfalls eine technische Dimension, denn wenn ein Zweck auch mit „milderen" technischen Mitteln erreicht werden kann, also technisch bedingt weniger Eingriffe in Grundrechte nötig sind, so ist das mildere Mittel zu wählen und das aktuell betrachtete Mittel nicht einzusetzen. Um zu evaluieren, ob es ein milderes Mittel gibt bzw. was ein milderes Mittel sein kann, ist unter Umständen technische Expertise vonnöten. An dieser Stelle sei auch auf Artikel 25 DSGVO (Datenschutz durch Technikgestaltung) verwiesen, der grundsätzlich alle Datenverarbeitungen verpflichtet, Technologien dem Stand der Technik entsprechend zu Erreichung eines Zwecks nur datensparsam und grundrechtsschonend einzusetzen.

Zweck A: Der Einsatz von Nahbereichstechnologien wie etwa Bluetooth könnte erforderlich sein, wenn etwa die Gesundheitsämter die Infektionsketten nicht mit anderen Mitteln schnell und effizient aufdecken können und eine App hinreichend erfolgversprechend scheint.

Zweck B: Für die allgemeine Überprüfung der Einhaltung von Ausgangsbeschränkungen sind keinerlei Einzeldaten mit Personenbezug notwendig, wodurch nur aggregiert-statistische Daten als milderes Mittel in Frage kommen. Detailliertere Daten,

wie beispielsweise konkrete Kontaktereignisdaten, individuelle GPS-Messungen oder andere Ortsdaten scheiden an dieser Stelle aus, da sie allein schon mit Blick auf Datenschutz eingriffsintensiver aber nicht hilfreicher sind.

Angemessenheit

An dieser Stelle müssen diverse Implikationen abgewogen werden, in diesem Beispiel sogar gesamtgesellschaftliche Auswirkungen. Das können medizinische Fragestellungen sein, aber auch soziale, wirtschaftliche oder psychologische, wobei auch diese jeweils miteinander verbunden sind. Es steht jedenfalls fest, dass **Zweck A** technisch gesehen – wenn überhaupt – mit Nahbereichstechnologien begegnet werden kann. Dabei steckt auch hier der Teufel im technischen Implementationsdetail. **Zweck B** hingegen darf technisch gesehen allein mit aggregierten Daten umgesetzt werden. Es ist jedenfalls nicht möglich, darüber hinaus Pauschalaussagen zu machen, denn es hängt ganz wesentlich von der konkreten technischen Implementierung ab, wie tief der jeweilige Eingriff in die Grundrechte ist, wie die aktuelle Diskussion um das PEPP-PT-Framework[1] und die dezentralisierte DP-3T-Implementation[2] zeigt.

Nicht zuletzt ist es dann relevant, ob das konkrete Ergebnis des App-Einsatzes überhaupt im Verhältnis zu den eingeschränkten Rechten steht. Bei experimentellen Apps wie den Corona-Tracing-App-Entwürfen ist dies besonders heikel, ist deren Nutzen doch nach wie vor überhaupt nicht abschätzbar. Der aktuelle Fokus auf Apps als Heilsbringer scheint überhaupt sehr problematisch, ist doch ein – bislang nur theoretisch modellierter – Effekt erst bei Nutzung durch mindestens 60 %[3] der Bevölkerung zu erwarten. Erkenntnisse aus Singapur mögen dafür instruktiv sein, wo sich nur 13 % der Menschen die individualisierte TraceTogether-App installiert[4] hatten. Eine datenschutzfreundliche Ausgestaltung kann zwar wesentlich zur Erhöhung der Akzeptanz einer deutschen oder europäischen Lösung beitragen, doch ebenso motivieren auch die Notwendigkeit einer hohen Verbreitung zusammen mit der Drohung eines ansonsten länger andauernden Lockdowns. Genügt dies jedoch nicht, kommt dennoch keine „Corona-App-Pflicht" in Frage, denn der unklare Nutzen einer solchen App kann – wie oben hergeleitet – doch nur minimale Grundrechtseinschränkungen rechtfertigen. Wie sehr die jeweiligen App-Entwürfe wiederum in Grundrechte eingreifen, ist ebenso unklar, fehlt es doch bislang an detaillierten Analysen. Unklarer Nutzen trifft also auf unklaren Schaden, kein guter Stand.

Abschluss und Fazit

Nach diesem Schema müssen alle aktuellen und zukünftigen Technikanwendungen analysiert werden, nur so können Schnellschüsse und eine weitere Aushöhlung der Grundrechte verhindert werden. Dies gilt insbesondere in Notfällen wie der aktuellen Pandemie. Grundrechte gelten auch in Notsituationen oder besser gesagt: gerade in Notsituationen müssen die Grundrechte gelten.

Der gesellschaftliche Fetisch hin zu informationstechnischen Lösungen für komplexe Probleme scheint nach wie vor ungebrochen und allzu oft werden dadurch alternative Herangehensweisen in den Hintergrund gedrängt oder unnötig Hoffnung geschürt. Und schon wird die App zum „entscheidenden Schlüssel"[5]. Aus diesem Grund müssen wir gerade in Notlagen besonders wachsam sein und den schnellen Verlockungen einfacher technischer Lösungen für extrem komplexe soziale Probleme widerstehen. So könnte es etwa zur Pandemieeindämmung unter Betrachtung aller Umstände weit sinnvoller zu sein, die staatliche Bestrebung und Kommunikation auf Maskennutzung und Erhöhung der Testkapazität auszurichten und nicht zu viel Hoffnung auf brauchbare Hilfe durch eine Corona-Tracing-App zu schüren.

Anmerkungen

1 *https://www.pepp-pt.org/*
2 *https://github.com/DP-3T/documents*
3 *https://www.heise.de/tp/features/Koennen-wir-der-Corona-App-vertrauen-4700302.html*
4 *https://www.golem.de/news/corona-app-per-bluetooth-kontaktpersonen-von-infizierten-ermitteln-2003-147461.html*
5 *https://www.merkur.de/politik/coronavirus-app-handy-pflicht-ueberwachung-daten-infizierte-symptome-deutschland-tracing-zr-13635397.html*

Göde Both

Informatiklehre durch fachspezifische *Gender Open Educational Resources* bereichern

Die Angebote des Portals *Gendering MINT digital*

Die meisten Gleichstellungsstrategien an den Hochschulen im Bereich Informatik zielen darauf, die Anzahl der Frauen zu erhöhen und strukturelle Barrieren für Studentinnen und Wissenschaftlerinnen aufzubrechen. Für die dritte Ebene von Gleichstellung – die des Gender-Wissens und der Gender-Kompetenzen – gibt es bislang kaum zielgruppenspezifische, freie Lehr-/Lernmaterialien. An diesem Bedarf hat unser Projekt angesetzt. Auf dem Portal Gendering MINT digital[1] *gibt es ab sofort eine Reihe von Lerneinheiten als* Open Educational Resources (OER) *für die Verwendung in der Lehre oder zum Selbststudium.*[2]

Nur wenige zielgruppenspezifische Lehr-/Lernmaterialien vermitteln wissenschaftliches Gender-Wissen[3] und Gender-Kompetenzen an Informatikstudierende: *Brigitte Ratzer* und *Bente Knoll* haben ein allgemeines Lehrbuch[4] für den Bereich Ingeni-

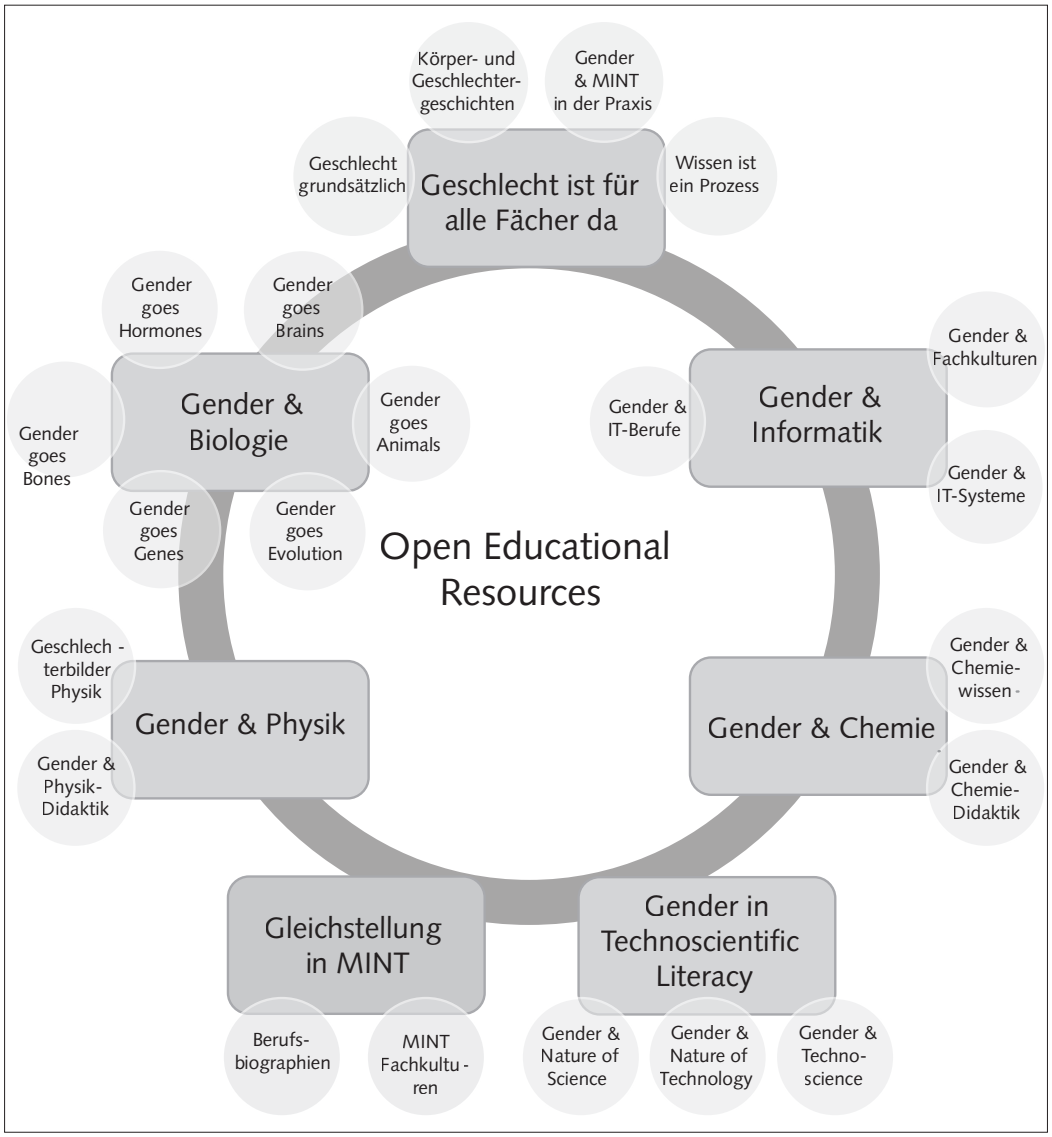
eurwissenschaften geschrieben, das auch auf die Spezifik von IT-Systemen und IT-Fachkulturen eingeht. Ende der 90er Jahre hat *Britta Schinzel* zusammen mit ihren KollegInnen ein Lehrbuch[5] für den Fernstudiengang *Informatik & Gesellschaft* veröffentlicht. Es ist heute leider nur noch antiquarisch oder in Bibliotheken erhältlich. Lehr-/Lernmaterialien, die auch gegenwärtige Diskussionen beispielsweise um Fachkulturen und *algorithmic bias* aufnehmen, gab es bislang nicht.

Das Portal Gendering MINT digital ist am Zentrum für transdisziplinäre Geschlechterstudien (ZtG) an der Humboldt-Universität zu Berlin angesiedelt. Es ist Teil eines Verbundprojektes der Uni Freiburg, der HU Berlin und der Hochschule Offenburg und wird durch das Bundesministerium für Bildung und Forschung (2018-2020) gefördert. Hinter dem Portal steht ein Team am ZtG aus WissenschaftlerInnen und StudentInnen mit Doppelqualifikationen in den MINT-Fächern und in den Gender Studies. Neben Informatik decken wir auch die naturwissenschaftlichen Fächer der Biologie, Chemie und Physik ab (siehe Grafik).

Unsere Open Educational Resources (OER) sind Lehr-/Lernmaterialien, die unter *creative-commons*-Lizenzen kostenlos genutzt und verbreitet werden können. Die OER sind strukturiert in sieben Lerneinheiten und verwenden einen Mix aus Videos, Animationen, illustrierten Texten sowie Rekapitulations- und Reflexionsübungen. Im Medien-Repositorium der Humboldt-Universität stehen die Projekterträge dauerhaft zur Verfügung. Auf unserem Portal[6] haben wir die OER zu Lerneinheiten gebündelt, wie *Gender & Informatik.* Diese Lerneinheit besteht wie auch die anderen Lerneinheiten aus mehreren Kapiteln: *Gender & IT-Berufe, Gender & Fachkulturen, Gender & IT-Systeme.* Informatiklehrende können die Lerneinheit nutzen, um fachbezogenes, wissenschaftliches Gender-Wissen in ihre Lehrveranstaltungen zu integrieren. Alternativ können interessierte Informatikleute unsere OERs auch zum Selbststudium verwenden.

Unsere Lerneinheiten und ihre Einsatzfelder

Die OER profitieren von einem reichhaltigen Schatz aus mehr als 40 Jahren Forschung und Lehre zu *Gender & MINT.* Für die Vermittlung in der Lehre stellen sie die komplexen Verhältnisse der Gender-Themen vereinfacht dar. Sie diktieren keine Unterrichtsmethode, sondern schlagen Einsatzmöglichkeiten der OER in der Lehre vor. Viele unserer Lerneinheiten sind modular aufgebaut, so dass einzelne Kapitel in beliebiger Reihenfolge verwendet werden können. Lehrende können die einzelnen Lerneinheiten je nach ihren konkreten Lehr-/Lernzielen verwenden, eigene Unterrichtsmethoden mit ihnen entwickeln oder auf didaktische Vorschläge in den Lerneinheiten des Portals zurückgreifen.[7]



Die Lerneinheiten (Rechtecke) und ihre Kapitel (Kreise) des Portals Gendering MINT digital

Die OER eröffnen Informatikstudierenden neue Sichtweisen auf ihr Fach und die IT-Berufswelten. In Lehrveranstaltungen können die OERs zur Kontextualisierung der vermittelten Schwerpunkte beitragen, beispielsweise *Maschinelles Lernen* oder *Software-Technik.* In der Tabelle 1 finden Sie unsere Empfehlungen zur Integration in typische Lehrveranstaltungen.

Die Lerneinheit *Gender ist für alle Fächer da* führt in den Themenkomplex ein. Sie erläutert grundlegende Konzepte und Theorien der Gender Studies, die historische Wandelbarkeit der Geschlechterverhältnisse und Geschlechtermodelle, bietet kurze State-

	Empfohlene Kapitel aus Gendering MINT digital				
Lehrveranstaltungsbeispiele	*Geschlecht ist für alle Fächer da: alle Kapitel*	*Gender & Informatik: Gender & IT-Berufe*	*Gender & Informatik: Gender & Fachkulturen*	*Gender & Informatik: Gender & IT-Systeme*	*Gender in Technoscientific Literacy: Gender & Nature of Technology*
Einführung Informatik	X	X	X	X	
KI / Maschinelles Lernen	X			X	
Software-Technik	X	X		X	
Informatik im Kontext (Informatik & Gesellschaft)	X	X	X	X	X
Mensch-Maschine-Interaktion	X	X		X	X
Informatikdidaktik (Informatik & Bildung)	X		X		X

Tabelle 1

ments von NaturwissenschaftlerInnen zu Gender-Themen in ihren Feldern und liefert Einführungen in die feministische Wissenschaftsforschung. Die Kapitel der Lerneinheit *Gender & Informatik* vermitteln anschaulich, wie Geschlecht und Informatik ko-konstruiert werden: in den Berufswelten der Software-Entwicklung, in den Selbst- und Fremdbildern der Informatik und in IT-Systemen. Das Kapitel *Gender & Nature of Technology* aus der Lerneinheit *Gender in Technoscientific Literacy* führt die bildungswissenschaftlichen Diskussionen um das Wesen der Technik mit Erkenntnissen aus den Gender Studies zusammen und eignet sich besonders für das Lehramt Informatik.

Teilen Sie uns ihre Erfahrungen mit!

Unsere OER wurden mit und von unseren ProjektpartnerInnen in der Biologie, Chemie, Informatik, Physik, Soziologie und im BA Gender Studies erprobt. Bis zum Ende der Projektlaufzeit (30. November 2020) werden die Erfahrungen und Rückmeldungen aus den Erprobungen in die Weiterentwicklung einfließen. Seien auch Sie Teil des Wandels zu mehr Geschlechtergerechtigkeit in der Informatik! Nutzen Sie unsere OER und teilen Sie uns ihre Erfahrungen aus ihrer Lehr-Praxis mit: *gemintdig.gender@hu-berlin.de*.

Anmerkungen

1 *https://www2.hu-berlin.de/genderingmintdigital/*
2 *Zum Zeitpunkt der Niederschrift des Beitrags waren noch nicht alle Lerneinheiten und Kapitel veröffentlicht.*
3 *Für eine Übersicht der geschlechtertheoretisch fundierten Gender-Lehre in den Technikwissenschaften: Bath, Corinna; Both, Göde; Lucht, Petra; Mauss, Bärbel; Palm, Kerstin (Hg.) (2017): rebootING. Handbuch Gender-Lehre in den Ingenieurwissenschaften. Berlin, Münster, Wien, Zürich, London: LIT Verlag.*
4 *Knoll, Bente/Ratzer, Brigitte (2010): Gender Studies in den Ingenieurwissenschaften. Wien: Facultas.wuv.*
5 *Schinzel, Britta/Parpart, Nadja/Westermayer, Till (1999): Informatik und Geschlechterdifferenz. Tübingen: Universität (Tübinger Studientexte Informatik und Gesellschaft).*
6 *https://www2.hu-berlin.de/genderingmintdigital/*
7 *Für eine Handreichung, die sich u. a. mit der Einbindung von Online-Bausteinen in die Präsenzlehre beschäftigt, siehe: Mayer, Veronika/Winheller, Sandra/Wedl, Juliette/Hofmeister, Arnd (2016): Handreichung zur Nutzung von E-Learning-Lehreinheiten in den Gender Studies. Band 1. Braunschweiger Zentrum für Gender Studies. DOI: 10.24355/DBBS.084-201608011055-0.*
8 *https://shop.budrich-academic.de/produkt/keeping-autonomous-driving-alive/*

Göde Both

Foto André Wunstorf

Göde Both arbeitet als wissenschaftlicher Mitarbeiter im Projekt *Gendering MINT digital* (Teilprojekt II am Zentrum für transdisziplinäre Geschlechterstudien an der Humboldt-Universität zu Berlin). Göde Both dankt Sigrid Schmitz für die konstruktiven Kommentare zu diesem Beitrag.
Göde Both *(https://goede-both.info)* ist Diplom-Informatiker und promovierter Sozialwissenschaftler. Seine Dissertation *„Keeping Autonomous Driving Alive: An Ethnography of Visions, Masculinity and Fragility"* erschien April 2020 bei Budrich Academic Press[8]. Sie eröffnet eine verstehend-kritische Perspektive auf informatischer Forschung, indem sie die Komplexität der Beziehungen zwischen Informatikern, ihren Visionen und ihren Artefakten entfaltet. Sie lässt sich als Lehrstück aus dem Feld Robotik und KI lesen.

Dominik Wetzel

Individualisierte Propaganda

Social Media und die Möglichkeiten gesetzlicher Kontrolle

Im Jahr 2004 gegründet, erreicht Facebook *inzwischen mehr als 2,7 Milliarden Menschen, auch über* WhatsApp *und* Instagram*. Für viele ist Facebook die zentrale Seite für Nachrichten, Werbung und Informationen über das Leben ihrer Freunde und Vorbilder. Milliarden nutzen* Google *und seine Tochterfirma* YouTube*. Die großen Plattformen haben eine außerordentliche Stellung im weltweiten Meinungskampf erreicht. Allein in Deutschland nutzen mehr als 30 Millionen Menschen Facebook.*[1]

Das ist gefährlich, wie der Fall um Cambridge Analytica *zeigt. Mithilfe von Algorithmen war es möglich, unzählige Persönlichkeitsprofile zu sammeln, um den Nutzerinnen und Nutzern auf sie zugeschnittene Informationen zukommen zulassen, die ihr Bild von der Wirklichkeit beliebig beeinflussen konnten.*

Beeinflussung der Nutzer

Facebooks algorithmische Redakteure

Der *News Feed* steht im Kern von Facebooks Erfolg. Das zunächst umstrittene Produkt hat sich zur wertvollsten Werbetafel der Welt entwickelt. Automatisierte Software verfolgt die Aktionen jedes Benutzers und liefert personifizierte Beiträge. Mit dem News Feed nimmt Facebook mehr ein als mit jedem anderen Teil der Website.[2] Jedes Mal, wenn man Facebook öffnet, tritt Facebooks Algorithmus in Aktion. Er sagt voraus, ob Nutzer die Schaltfläche *Gefällt mir* für einen Beitrag drücken, auf Inhalte klicken, sie kommentieren, freigeben, ausblenden oder als Spam markieren.

Die erste Anzeige wurde unter Tausenden gewählt, diejenige zu sein, mit der Nutzer am ehesten interagieren, oder die sie emotional berührt.[3] Dazu hierarchisiert der Algorithmus zwischen 1500 und 10 000 *Posts*. Um sicherzustellen, dass die ersten 300 Beiträge interessanter sind als alle anderen, verwendet Facebook Tausende von Faktoren, um festzustellen, was im Feed einer Benutzerin oder eines Benutzers erscheint. Er scannt und sammelt alles, was in der letzten Woche von Freunden, jedem, dem man folgt, jeder Gruppe, zu der man gehört, und jeder *gelikten* Facebook Seite gepostet wurde.[4] Basis ist Facebooks KI *FBLearner Flow.* Sie wird mit persönlichen Daten der Nutzer gefüttert und führt Simulationen anhand eines Entscheidungsbaums durch, um unterschiedliches Kundenverhalten vorherzubestimmen. Aus den Ergebnissen erstellt Facebook Gruppen von Charakteren, die sich ähnlich verhalten. Unternehmen/Organisationen können diese Personengruppen mit Werbung ansprechen, um gewünschte Verhalten zu fördern.[5] Der Algorithmus kann identifizieren, welche Posts die meiste Aufmerksamkeit bekommen und *viral gehen*, und wie und wann eine Nachricht dazu gesetzt werden muss. Auch Verleger und Werbetreibende machen sich die Taktiken zu eigen.[6]

Suchtpotenzial

Facebook verdient umso mehr Geld, je mehr Zeit die Nutzer auf der Plattform verbringen, genau wie andere Firmen. Sie tun ihr Möglichstes, damit sich die Nutzer auf den Websites wohlfühlen. Es hat sich herausgestellt, dass sich das bloße Konsumieren von Informationen negativ auf das Wohlbefinden von Menschen auswirkt, während diejenigen, die posten und mit anderen Nutzern interagieren, sich danach besser fühlen.[7] Die Websites sind so gestaltet, dass bei den Besuchern regelmäßig Dopamin ausgeschüttet wird, was die Nutzer abhängig macht.[8] Nach einer repräsentativen Studie von 100 000 Befragten verbringen in Deutschland rund 85 % der 12- bis 17-Jährigen durchschnittlich drei Stunden pro Tag auf sozialen Netzwerken. 2,6 % davon zeigen ein Suchtverhalten.[9] Junge Erwachsene verbringen durchschnittlich täglich mehr Zeit mit der Nutzung sozialer Medien als irgendeiner anderen Aktivität.

Facebooks Gründungspräsident *Sean Parker* kritisierte, dass das Unternehmen die Verletzlichkeit der menschlichen Psyche ausnutze, um eine Feedbackschleife der sozialen Wertschätzung herzustellen, die die Nutzer an die Plattform bindet.[10] Der ehemaliger Vizepräsident *Chamath Palihapitiya* mahnte 2011 sogar, diese kurzfristigen, Dopamin-gesteuerten Feedbackschleifen würden die Funktionsweise der Gesellschaft, den zivilen Diskurs und Kooperation zerstören und helfen, Fehlinformationen zu verbreiten. *Justin Rosenstein,* Erfinder des *Like Buttons,* warnte vor einem Internet, das um die Wünsche der Werbeindustrie herum gestaltet wird.[11]

Filterblasen

Interessen und Meinungsbild des Nutzers bestimmen die Auswahl der Suchergebnisse, so dass bei Suchanfragen ständig sich ähnelnde Informationen hervorgebracht werden. Das ist den meisten Nutzern nicht bewusst, was die in einem demokratischen Prozess notwendige kritische Auseinandersetzung mit der eigenen Meinung erschwert und zur Polarisierung der Bevölkerung beitragen kann.[12] Der Algorithmus geht davon aus, dass Inhalte, die viele Interaktionen hervorgerufen haben, großen Anklang finden, sie werden daher in den Feeds von mehr Menschen platziert.[13] Der Journalist *Eli Pariser* befürchtet nicht nur politische Polarisierung sondern Verdummung. Da sich die meisten Menschen kaum für Politik interessieren, folgen sie selten entsprechenden Links. Dies registrieren Facebooks Algorithmen und priorisieren dementsprechend Hochzeitsfotos oder Katzenvideos gegenüber Nachrichten.[14]

Rohingya

Dieses Prinzip beeinflusste die *ethnischen Säuberungen* an der muslimischen Rohingya-Minderheit in Myanmar.[15] Facebook ist dort der am stärksten genutzte Zugang zum Internet mit 30 Mil-

lionen Nutzern bei einer Bevölkerung von 55,6 Millionen.[16] Damit sind Facebooks Algorithmen zentral für die Informationsversorgung von mehr als der Hälfte der Burmesen.[17] Militärs in Myanmar machten sich daran, Facebook-Seiten zu nutzen, die von vielen *geliked* werden sollten. Diese Seiten von Popstars, Models und Berühmtheiten, die zunächst keinen politischen Bezug hatten, begannen nach einiger Zeit, sich dem Militär zugeneigt zu äußern und verbreiteten später diffamierende Fotos, aufhetzende Posts und Falschnachrichten über die muslimische Minderheit. Vom Militär geführte *Troll*-Konten halfen dabei, den Inhalt zu verbreiten, beschimpften Kritiker und schürten Streit zwischen Kommentatoren. Oft posteten sie Bilder von Leichen als angebliche Hinweise auf von Rohingya verübte Massaker.[18] Das Aufhetzen der Bevölkerung eskalierte 2017. Das burmesische Militär verübte schwere Menschenrechtsverbrechen gegen die Minderheit.[19]

Facebook löschte später 425 Seiten, 17 Gruppen und 135 Konten, die zunächst auf Unterhaltung ausgerichtet, jedoch eng mit dem Militär verbunden waren und teilweise etwa 2,5 Millionen *Follower* hatten.[20]

Gewährleistung freier Meinungsäußerung

Dadurch, dass die großen Meinungsplattformen wie Google, Facebook und Twitter in verschiedensten Teilen der Welt aktiv sind, kommt ihnen eine Sonderrolle für die freie Meinungsäußerung zu.[21] Regierungen regulieren sie durch Richtlinien, die Plattformen sich selbst durch Codes und Normen.[22] Nutzer mögen diese Richtlinien akzeptieren, kennen sie aber kaum. Oft werden sie gesperrt, ohne die Möglichkeit sich zu rechtfertigen.[23] Von den Betreibern geahndete Äußerungen würden normalerweise durch Art. 5 I Grundgesetz (GG) geschützt. Die Regeln, die Plattformbetreiber setzen, sind deutlich enger.[24]

Strategien alter Schule wenden traditionelle strafrechtliche Mittel oder Zensur gegen die Sprecher an, *New-School*-Regulierung betrifft die Infrastruktur, Websiteprovider, Social Media Plattformen und dergleichen.[25] Löschen die Betreiber die Inhalte nicht, zieht sie der Staat zur Verantwortung.[26] Regierungen betreiben weiter die Methoden alter Schule, zunehmend jedoch auch New-School-Taktiken.[27] Facebook gibt an, zwischen Oktober 2017 und März 2019 99,8 % des Spams entfernt zu haben, noch bevor die Nutzer dies gemeldet hätten. Von Januar bis März 2019 lag der Anteil der noch nicht gemeldeten, jedoch schon gelöschten Gewaltdarstellung bei 98,9 %, die Zahl der gelöschten terroristischen Propaganda liegt seit Januar 2018 bei über 99,3 %.[28] Zwar unterstützt KI das Löschen von Inhalten, die Hauptarbeit machen aber Menschen in Niedriglohnländern wie den Philippinen, Irland, Mexiko, Türkei oder Indien. Sie schauen sich Tausende problematische Videos und Bilder am Tag an und entscheiden, ob die Inhalte zensiert werden oder auf der Plattform bleiben.[29]

Community (Gemeinschafts-)*Standards*

Facebook geht offensiv gegen Hassrede vor. Die Gemeinschafts-Standards schützen bestimmte Bevölkerungsgruppen besonders vor Einschüchterungen und direkten Angriffen aufgrund von ethnischer Zugehörigkeit, Religion, Erkrankung oder sexueller Orientierung.[30] Mittlerweile werden gemäß Facebooks Gemeinschafts-Standards Inhalte entfernt, die Gewalt, Erniedrigung oder Leid anderer verherrlichen. Das Unternehmen erkennt aber die Notwendigkeit an, über Menschenrechtsverletzungen aufzuklären.[31] Dennoch wurden Posts und Konten von Rohingya-Aktivisten gelöscht, weil sie Gewalt gegen die Minderheit zeigten. YouTube-Konten, die über die Gewalt aufklärten, wurden gelöscht.[32] Plattformen müssen unterscheiden zwischen *Fake News* und Satire, Gewaltvideos und Journalismus, zwischen dem Glorifizieren und dem Aufdecken von Verbrechen. Dies führt häufig zu Problemen, wie im Fall eines Videos aus einem ägyptischen Foltergefängnis, das von YouTube gelöscht wurde, da es gegen die Nutzungsbedingung verstieß. Damit trug die Plattform kurzzeitig zum Vertuschen von Verbrechen bei, bis sie das Video wieder zuließ.[33]

Terroristische Propaganda

Eine weitere Gefahr für die Meinungsfreiheit ist das Kategorisieren als terroristische Propaganda. So definiert die türkische Regierung die *PKK* (Kurdische Arbeiterpartei) und deren bewaffneten Arm als Terrororganisation.[34] Die EU hat sich dieser Einschätzung angeschlossen.[35] Bei der PKK handelt es sich jedoch nach wie vor um die bedeutendste Kurdenorganisation mit den meisten Mitgliedern.[36] Belgische Gerichte stufen sie heute nicht mehr als Terrororganisation ein, sondern als Partei in einem bewaffneten Konflikt.[37] Facebook deutet Darstellungen der PKK oder ihres Gründers *Abdullah Öcalan* als nach den Gemeinschafts-Standards verbotene terroristische Propaganda und zensiert damit beispielsweise Unterstützerinnen der kurdischen Unabhängigkeitsbewegung.[38]

Ein Großteil des weltweiten Informationsaustauschs findet auf Plattformen wie Facebook, Google und Twitter statt und diese passen sich der Deutungshoheit von Regierungen an. Regime können so Meinungen durch Zensur unsagbar machen und die Plattformen gestalten die öffentliche Debatte im Sinne des politischen Status quo.

Cambridge Analytica

Cambridge Analytica (CA) hatte auf den Wahlkampf um die US-amerikanische Präsidentschaft sowie den *Brexit*-Volksentscheid eingewirkt.[39] Die Taktik ist die des Micro-Targeting. Hierzu teilt man die Zielgruppe anhand von unterschiedlichen Mustern in verschiedene Personengruppen auf, denen man einem gemeinsamen Nenner angepasste Informationen zukommen lässt, um ihr Handeln zu beeinflussen.

2017 begannen die Enthüllungen. CA behauptete, Zugang zu den Facebook-Profilen von 230 Millionen amerikanischen Wählern zu haben. Der spätere Whistleblower *Christopher Wylie* sprach davon, dass sie Tausende persönliche Informationen aus den Nutzerprofilen zusammentrugen: von der religiösen Einstellung über Medikamente und ob die Nutzerinnen und Nutzer ein Auto besaßen oder nicht, bis hin zur politischen Ausrichtung und den Lieblings-TV-Sendungen. Sie flossen in die Modelle ein, mit denen sich die Nutzer kategorisieren ließen.[40] Das System,

auf dem später CAs Strategie fußen sollte, erarbeitete der Psychologe *Michal Kosinski* mit seinem Team. Das *OCEAN*-Modell *(Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism)* kategorisiert nach Aufgeschlossenheit, Gewissenhaftigkeit, Extrovertiertheit, Verträglichkeit und Neurotizismus.[41] Nach diesem Grundgerüst erstellte *Aleksandr Kogan* von der Cambridge Universität eine Persönlichkeits-App, mit der Nutzer ihre Psyche definieren konnten. Kogans Quiz hatte zwar nur etwa 300 000 Teilnehmer, insgesamt waren aber rund 87 Millionen Facebook-Nutzer betroffen. Kogan griff mit seiner App nicht nur auf die Profile der Nutzer zu, sondern auch auf deren Freunde, obwohl diese den App-Bedingungen nie zugestimmt hatten. Damit kam schnell ein gewaltiger Datensatz zustande, den er später an CA verkaufte.[42]

Kosinski und sein Team warnten, dass die Facebook-Likes Vorhersagen ermöglichen, mit denen Unternehmen, Regierungen oder Facebook-Freunde Rückschlüsse auf die Intelligenz, sexuelle Orientierung und politische Ansichten ziehen können. Das kann erhebliche Folgen haben. Kogan erklärte später, dass er 30 Millionen Nutzerprofile an CA weitergab. Die Berichte, wie viele Nutzer tatsächlich betroffen waren, schwanken zwischen mehreren Dutzend Millionen.[43]

Die ersten Schritte im US-Wahlkampf machte CA an der Seite des republikanischen Kandidaten *Ted Cruz.*[44] Die Kampagne sollte Menschen auf emotionaler Ebene ansprechen, um ihre Zustimmung auf funktionaler Ebene zu bekommen, und verfolgte eine Strategie, die sich um Immigrationsängste, Haltungen gegen die Regierung und eine Vorliebe für starke Anführer drehte.[45] Da von vielen Tausenden Wählern die Persönlichkeitsprofile vorlagen, konnte diese dann gezielt mit „überzeugenden" Nachrichten bespielt werden, um sie „weiter nach rechts zu bewegen".[46] Eine Kampagne konnte Haushalte und Einzelpersonen gezielt ansprechen. Knapp neunzig Millionen Facebook-Nutzer sind vermutlich durch den Cambridge- Analytica-Skandal betroffen. Auch Twitter hat Daten an Kogan und *Global Science Research* weitergegeben, es liegen keine genauen Angaben vor, wie viele Betroffene es gab.[47] Auch wenn manche den Einfluss von CA auf das Wählerverhalten deutlich anzweifeln,[48] war Cruz zu der Zeit, in der sie seinen Wahlkampf unterstützten, der stärkste innerparteiliche Konkurrent Trumps.[49]

Gegenmaßnahmen

Für die US-Wahlen 2020 hat Facebook strengere Regeln vorgegeben, die Verantwortlichen einer Seite offenzulegen, und sperrt Werbung, die Wähler von der Urne fernhalten soll.

Vertragliche Maßnahmen

Medienrecht geht vom Menschenbild einer umfassend informierten Bürgerin aus, die verschiedene Ansichten gegeneinander abwägen und selbstbestimmt eine Wahl treffen kann. Um eine einseitige Information der Bevölkerung zu verhindern, gilt der Rundfunkstaatsvertrag (RStV) für die herkömmlichen Medien wie die öffentlich-rechtlichen Sender. § 11 II des RStV beauftragt die öffentlich-rechtlichen Rundfunkanstalten

> *„bei der Erfüllung ihres Auftrags die Grundsätze der Objektivität und Unparteilichkeit der Berichterstattung, die Meinungsvielfalt sowie die Ausgewogenheit ihrer Angebote zu berücksichtigen."*

Im Laufe diesen Jahres soll der Staatsvertrag auch Online-Streamingdienste und Social-Media-Plattformen einbeziehen. Sie werden verpflichtet, transparent darzustellen, nach welchen Kriterien sie Inhalte präsentieren, und dürfen die Auffindbarkeit journalistisch-redaktionell gestalteter Angebote nicht ohne sachlich gerechtfertigten Grund behindern.[50]

Damit sich die Ereignisse um CA nicht wiederholen, haben sich Facebook, Google, Twitter und Mozilla sowie Vertreter der Werbeindustrie im September 2018 der EU Kommission gegenüber verpflichtet, gegen Falschmeldungen im Internet vorzugehen.[51] Dazu müssten Falschmeldungen erkennbar sein und deren Verfasser müssten identifiziert und überwacht werden. Nach eigenen Angaben ist sich Facebook bewusst, dass zwischen Falschmeldungen und Satire oder Meinungen nur ein schmaler Grat liegt. Es entfernt Falschmeldungen nicht, sondern reduziert ihre Verbreitung, indem sie weiter unten im News Feed angezeigt werden.[52] Trotzdem ist die Gefahr groß, sich dadurch eine Deutungshoheit über die Wahrheit anzumaßen.

Gesetzliche Maßnahmen

Das Grundrecht der Meinungsfreiheit gibt jedem das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten. Ein Eingriff in die Meinungsfreiheit liegt in jeder staatlichen Regelung oder Entscheidung, die die Äußerung oder Verbreitung von Meinungen verbietet, erschwert oder durch Sanktionen verhindert.[53] Blockiert eine Behörde beispielsweise einen Facebook- oder Twitter-Beitrag, handelt es sich um einen Eingriff in die Meinungsfreiheit, weil die/der Blockierte nicht mehr kommentieren kann und so aus dem öffentlichen Diskurs ausgeschlossen wird.

Das NetzDG verpflichtet große soziale Netzwerke mit zwei Millionen oder mehr registrierten Nutzern im Inland zu einem wirksamen und transparenten Verfahren für Beschwerden über rechtswidrige Inhalte. Das Verfahren muss gem. § 3 I-III NetzDG unter anderem „gewährleisten", dass der Anbieter des Netzwerks „offensichtlich rechtswidrige Inhalte" grundsätzlich innerhalb von 24 Stunden und alle sonstigen rechtswidrigen Inhalte innerhalb von sieben Tagen löscht oder sperrt. Der Verstoß gegen diese Pflicht kann nach § 4 II NetzDG mit einem Bußgeld von bis zu 5 Millionen Euro geahndet werden.[54]

In seiner Entscheidung zur Partei *III. Weg* stützt sich das Bundesverfassungs-Gericht (BVerfG) darauf, dass Facebook gemäß § 1 III NetzDG iVm. § 130 StGB verpflichtet gewesen sei Maßnahmen zu ergreifen. Die Äußerungen der Partei qualifizierten sich als Volksverhetzung. Hätte Facebook nicht gehandelt, läge darin ein Verstoß gegen die Pflichten des Plattformbetreibers, der mit Geldbußen nach § 4 NetzDG belegt ist.[55]

Nach Art. 6 I Datenschutz-Grundverordnung (DSGVO) bedürfen grundsätzlich alle Datenverarbeitungen entweder einer gesetzlichen Grundlage oder der Einwilligung der Betroffenen.[56] Mit der DSGVO gehen nun die Datenschutzbehörden europa-

weit gegen große Unternehmen vor. Die Praxis der Persönlichkeitsauswertung, die den Grundstein zu CAs Machenschaften gelegt hat, verhindert aber auch die DSGVO nicht.

Gegen Google hat die französische Datenschutzbehörde 50 Millionen Euro Strafe verhängt, sie begründet die Strafe mit der Art und Weise, wie Google über die Nutzung von personenbezogenen Daten informiert. Google verstoße gegen die DSGVO, da die Informationen nur schwer zugänglich und in einigen Punkten unklar seien. Außerdem sei der Zweck der Datenerhebung zu allgemein und vage beschrieben.[57]

Fazit

Wie schon Kosinski und sein Team feststellten, stecken ungeahnte Gefahren in der Informationssammlung über Milliarden von Menschen. Nicht nur für die Unversehrtheit der Nutzer, sondern auch für die Demokratie. Das Geschäftsmodell der Onlineplattformen beruht auf Werbung und Facebooks außerordentlicher Fähigkeit, Nutzer zu analysieren und zu manipulieren. Big Data kann nie dagewesene Einsichten in menschliches Verhalten erlangen. Dies kann der Vorhersage, dem Risikomanagement, aber auch der Bevölkerungskontrolle dienen.[58] Viele gesellschaftliche Probleme können durch soziale Medien verstärkt werden. Einige lassen sich durch Reformen beheben, andere Fehler liegen im Geschäftsmodell. Die Handhabung von Big Data zeigt Machtasymmetrien. Die Plattformen sammeln sensible Informationen über die Nutzer. Diese werden dadurch durchsichtig, die Betreiber aber nicht. Es gilt also, die informationelle Selbstbestimmung auch gegenüber Privatunternehmen aufrecht zu erhalten und neue Strukturen zu schaffen, die verhindern, dass psychologische Profile von Kunden erstellt und verkauft werden.

Anmerkungen

1 *Kaiser, Leon; „Bundestag überlegt, digitale Plattformen zur Öffnung zu verpflichten", Netzpolitik, 28.4.2018; https://netzpolitik.org/2018/bundestag-ueberlegt-digitale-plattformen-zur-oeffnung-zu-verpflichten/*

2 *Oremus, Will; "Who Really Controls What You See in Your Facebook Feed—and Why They Keep Changing It"; Slate, 3.1.2016; http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_s_news_feed_algorithm_works.html?via=gdpr-consent*

3 *Oremus, Will; "Who Really Controls What You See in Your Facebook Feed—and Why They Keep Changing It"; a. a. O.*

4 *Oremus, Will; "Who Really Controls What You See in Your Facebook Feed—and Why They Keep Changing It"; a. a. O.*

5 *Biddle, Sam; "Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document"; The Intercept, 13.4.2018 https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/*

6 *Oremus, Will; "Who Really Controls What You See in Your Facebook Feed—and Why They Keep Changing It"; Slate, 3.1.2016; http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_s_news_feed_algorithm_works.html?via=gdpr-consent*

7 *FB Newsroom, "Hard Questions: Is Spending Time on Social Media Bad for Us?" Facebook Newsroom, 15.12.2017 https://newsroom.fb.com/news/2017/12/hard-questions-is-spending-time-on-social-media-bad-for-us/; Hern, Alex, "'Never get high on your own supply' – why social media bosses don't use social media", The Guardian, 23.1.2018 https://www.theguardian.com/media/2018/jan/23/never-get-high-on-your-own-supply-why-social-media-bosses-dont-use-social-media*

8 *WHO, "Public Health Implications of Excessive Use of the Internet, Computers, Smartphones and Similar Electronic Devices Meeting Report", 2014, S.79 ff.*

9 *Zeit Online, „Drei Stunden am Tag sind normal", 1.3.2018 https://www.zeit.de/digital/internet/2018-03/social-media-dak-studie-instagram-whatsapp-sucht-jugendliche*

10 *Wong, Julia Carrie, "Former Facebook executive: social media is ripping society apart", The Guardian, 12.12.2017, https://www.theguardian.com/technology/2017/dec/11/facebook-former-executive-ripping-society-apart; Allen, Mike, "Sean Parker unloads on Facebook: "God only knows what it's doing to our children's brains"", Axios, 9.11.2019, https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html*

11 *Lewis, Paul, "'Our minds can be hijacked': the tech insiders who fear a smartphone dystopia", The Guardian, 6.10.2017, https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia*

12 *Dörr, Dieter; Natt, Alexander, „Suchmaschinen und Meinungsvielfalt", Zeitschrift für Urheber und Medienrecht, 2014 Heft 11, 829 (837)*

13 *Luckerson, Victor, "Here's How Facebook's News Feed Actually Works", Time, 9.7.2015, https://time.com/collection-post/3950525/facebook-news-feed-algorithm/*

14 *Hurtz, Simon; Tanriverdi, Hakan, „Filterblase? Selbst schuld!" Süddeutsche, 2.5.2017, https://www.sueddeutsche.de/digital/facebook-filterblase-selbst-schuld-1.3479639*

15 *Mozur, Paul, "A Genocide Incited on Facebook, With Posts From Myanmar's Military", New York Times, 15.10.2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html*

16 *CIA World Factbook, "Burma Transnational Issues", Central Intelligence Agency, The World Factbook, 2018, https://www.cia.gov/library/publications/the-world-factbook/geos/bm.html*

17 *Spohr, Frederic, „Was Facebook mit der Vertreibung der Rohingya zu tun hat", Handelsblatt, 13.3.2018, https://www.handelsblatt.com/politik/international/myanmar-was-facebook-mit-der-vertreibung-der-rohingya-zu-tun-hat/21065446-all.html?ticket=ST-66238251-SHAUZnq933uRbTqhpixp-ap5*

18 *Mozur, Paul, "A Genocide Incited on Facebook, With Posts From Myanmar's Military", New York Times, 15.10.2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html*

19 *HRW, Rohingya Crisis, Human Rights Watch, 2019, https://www.hrw.org/tag/rohingya-crisis*

20 *FB-Newsroom, "Removing Myanmar Military Officials From Facebook", 28.8.2018, https://newsroom.fb.com/news/2018/08/removing-myanmar-officials/; Mozur, Paul, "A Genocide Incited on Facebook, With Posts From Myanmar's Military", New York Times, 15.10.2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html*

21 *Balkin, Jack, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation", HeinOnline, Davis University of California, 2018, 1149 (1182)*

22 *Balkin, Jack, a. a. O. (1187)*

23 *Balkin, Jack, a. a. O. (1197)*

24 *Balkin, Jack, a. a. O. (1194f.)*

25 *Balkin, Jack, a. a. O. (1174)*

26 *Balkin, Jack, a. a. O. (1175ff.)*

27 *Balkin, Jack, a. a. O. (1175)*

28 *FB-Newsroom, "Facebook's Community Standards Enforcement Report", An Update on How We Are Doing At Enforcing Our Community*

Standards, 23.5.2019, https://newsroom.fb.com/news/2019/05/enforcing-our-community-standards-3/

29 *Naughton, John, "Facebook's burnt-out moderators are proof that it is broken", The Guardian, 6.1.2019, https://www.theguardian.com/commentisfree/2019/jan/06/proof-that-facebook-broken-obvious-from-modus-operandi; Klonick, Kate, "The New Governors: The People, Rules, and Processes governing online Speech", Harvard Law Review, Vol. 131, 2018, 1598 (1640)*

30 *Facebook, „Teil III, Anstößige Inhalte", Gemeinschaftsstandards, Facebook, 2019, https://de-de.facebook.com/communitystandards/objectionable_content*

31 *Facebook, „Teil III, Gewalt", Gemeinschaftsstandards, Facebook, 2019, https://de-de.facebook.com/communitystandards/graphic_violence*

32 *BBC, "Why are posts by Rohingya activists getting deleted?", BBC Trending, 23.9.2017, https://www.bbc.com/news/blogs-trending-41364633*

33 *Klonick, Kate, "The New Governors: The People, Rules, and Processes governing online Speech", Harvard Law Review, Vol. 131, 2018, 1598 (1619f.)*

34 *CIA World Factbook, "Turkey Terrorism", Central Intelligence Agency, The World Factbook, 2018, https://www.cia.gov/library/publications/the-world-factbook/geos/tu.html*

35 *Amtsblatt der Europäischen Union, Beschluss des Rates 2017/1426; L 204/97, 5.8.2017, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2017:204:FULL&from=DA*

36 *Baden Württemberg Landesamt für Verfassungsschutz, „Arbeiterpartei Kurdistans" (PKK), Landesamt für Verfassungsschutz, Baden Württemberg, https://www.verfassungsschutz-bw.de/,Lde/Startseite/Arbeitsfelder/Kurden_PKK*

37 *Reuters, "Turkish foreign ministry summons Belgium's ambassador in Ankara", Reuters, 11.3.2019, https://www.reuters.com/article/us-turkey-security-belgium/turkish-foreign-ministry-summons-belgiums-ambassador-in-ankara-idUSKBN1QS1JL*

38 *Hern, Alex, "Publisher's Facebook page deleted after posting criticism of Turkish government", The Guardian, 13.5.2016, https://www.theguardian.com/technology/2016/may/13/facebook-turkish-government-zed-books*

39 *Grassegger, Hannes; Krogerus, Mikael, „Ich habe nur gezeigt, dass es die Bombe gibt", Das Magazin N°48 – 3.12.2016, https://web.archive.org/web/20170127181034/https:/www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/*

40 *Kroll, Andy, "Cloak and Data: The Real Story Behind Cambridge Analytica's Rise and Fall", MotherJones, Mai/Juni 2018, https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analytica-robert-mercer/*

41 *Bachrach, Yoram; Kosinski, Michal; Graepel, Thore; Pushmeet, Kohli; Stillwell, David, "Personality and Patterns of Facebook Usage", WebSci '12 Proceedings of the 4th Annual ACM Web Science Conference, Pages 24-32, 22.6.2012, https://dl.acm.org/citation.cfm?id=2380722*

42 *Davies, Harry; "Ted Cruz using firm that harvested data on millions of unwitting Facebook users", The Guardian, 11.12.2015, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data*

43 *Vincent, James, "Academic who collected 50 million Facebook profiles: 'We thought we were doing something normal'", The Verge, 21.3.2018, https://www.theverge.com/2018/3/21/17146342/facebook-data-scandal-cambridge-analytica-aleksandr-kogan-scapegoat*

44 *Davies, Harry; "Ted Cruz using firm that harvested data on millions of unwitting Facebook users", The Guardian, 11.12.2015, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data*

45 *Kroll, Andy, "Cloak and Data: The Real Story Behind Cambridge Analytica's Rise and Fall", Mother Jones, Mai/Juni 2018, https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analytica-robert-mercer/*

46 *"Cambridge Analytica – The Power of Big Data and Psychographics", Concodria, YouTube, 27.9.2016, 7:00, https://www.youtube.com/watch?v=n8Dd5aVXLCc&feature=youtu.be&t=420*

47 *Kurz, Constanze, „Cambridge Analytica wieder in den Schlagzeilen: Datenabgriff auch von Twitter", Netzpolitik.org, 30.4.2018, https://netzpolitik.org/2018/cambridge-analytica-wieder-in-den-schlagzeilen-datenabgriff-auch-von-twitter/*

48 *Taggart, Kendall, "The Truth About The Trump Data Team That People Are Freaking Out About", BuzzFeed News, 16.2.2017, https://www.buzzfeednews.com/article/kendalltaggart/the-truth-about-the-trump-data-team-that-people-are-freaking*

49 *Grassegger, Hannes; Krogerus, Mikael, "Ich habe nur gezeigt, dass es die Bombe gibt", Das Magazin N°48 – 3.12.2016, https://web.archive.org/web/20170127181034/https:/www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/*

50 *Tagesschau, „Medienstaatsvertrag – Grundregeln für die digitale Welt, 5.12.19, https://www.tagesschau.de/inland/medienstaatsvertrag-rundfunkstaatsvertrag-101.html*

51 *EU Commission, «Code of Practice on Disinformation», 26.9.2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation*

52 *Facebook, „Teil IV, Falschmeldungen", Gemeinschaftsstandards, 2019, https://de-de.facebook.com/communitystandards/false_news*

53 *Jacobsen, Annika; Kalscheuer, Fiete, „Das digitale Hausrecht von Hoheitsträgern", Neue Juristische Wochenschrift, 2018, 2358 (2359)*

54 *Hong, Mathias, „Das NetzDG und die Vermutung für die Freiheit der Rede", Verfassungsblog, 9.1.2018, https://verfassungsblog.de/das-netzdg-und-die-vermutung-fuer-die-freiheit-der-rede/*

55 *BVerfG,1 BvQ 42/19 Rn. 5*

56 *Engeler, Malte, „Datenschutz, Meinungsfreiheit und das Strache-Video: der Gesetzgeber muss handeln", Verfassungsblog, 21.5.2019, https://verfassungsblog.de/datenschutz-meinungsfreiheit-und-das-strache-video-der-gesetzgeber-muss-handeln/*

57 *Rebiger, Simon; Dachwitz, Ingo, „Die DSGVO zeigt erste Zähne: 50-Millionen-Strafe gegen Google verhängt", Netzpolitik.org, 21.1.2019, https://netzpolitik.org/2019/die-dsgvo-zeigt-erste-zaehne-50-millionen-strafe-gegen-google-verhaengt/*

58 *Balkin, Jack, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation", HeinOnline, Davis University of California., 2018, 1149 (1157)*

Dominik Wetzel

Dominik Wetzel arbeitet als freier Journalist und studiert Politikwissenschaft und öffentliches Recht an der Universität Tübingen.

Hans-Jörg Kreowski

Aufruf zur Unterstützung der Zeitschrift Wissenschaft und Frieden

Die Zeitschrift Wissenschaft und Frieden (W&F) erscheint seit 1983 vierteljährlich. Sie berichtet regelmäßig zu friedenspolitischen, militär-strategischen und rüstungstechnischen Fragen, publiziert zu Gewaltursachen und -verhältnisses, thematisiert Möglichkeiten ziviler Konfliktlösung und der Wahrung der Menschenrechte und bezieht aus naturwissenschaftlicher, technikwissenschaftlicher, politikwissenschaftlicher, sozialwissenschaftlicher, psychologischer, juristischer und ethischer Sicht Position zur Verantwortung der Wissenschaft. W&F ist eine unverzichtbare Stimme in einer Zeit, in der in vielen Teilen der Welt Krieg geführt und weltweit schamlos aufgerüstet wird, während die völkerrechtliche Verpflichtung zum friedlichen Miteinander der Staaten, wie es in der UN-Charta vereinbart ist, weitgehend in Vergessenheit geraten zu sein scheint. Weitere Informationen können dem Werbebrief von Johannes M. Becker und Paul Schäfer entnommen werden (siehe Kasten).

Das FIfF gehört neben zehn anderen Organisationen (darunter Arbeitsgemeinschaft für Friedens- und Konfliktforschung, Arbeitskreis Historische Friedens- und Konfliktforschung, Bund demokratischer Wissenschaftlerinnen und Wissenschaftler, Forum Friedenspsychologie, Informationsstelle Militarisierung und Zentrum für Konfliktforschung) zum Herausgeberkreis von W&F. Nachdem Dietrich Meyer-Ebrecht viele Jahre lang das FIfF im Vorstand von W&F und ich im Beirat vertreten haben, sind vor zwei Jahren die Rollen getauscht worden. Mit Thomas Gruber hatte ein FIfF-Mitglied auch bis Ende 2019 zwei Jahre lang in der Redaktion mitgearbeitet. Leider hat sich bisher niemand gefunden, die oder der das fortführen mag. Auch inhaltlich trägt das FIfF einiges zu W&F bei. Neben Zeitschriftenbeiträgen sind mehrere Dossiers, von denen zwei bis drei pro Jahr dem Heft beiliegen, vom FIfF herausgegeben worden. Die Mitwirkung des FIfF halte ich für sehr wichtig, weil sie ein technikwissenschaftliches Gegengewicht zu der starken gesellschaftswissenschaftlichen Ausprägung bildet.

Das Erscheinen von W&F ist allerdings gefährdet, weil ihre Herausgabe seit einigen Jahren mehr kostet, als eingenommen wird, und die finanziellen Reserven zur Neige gehen. Es gibt große Anstrengungen, die Ausgaben zu senken. Aber das wird nicht reichen, wenn nicht auch die Einnahmeseite verbessert wird.

Ich möchte deshalb alle, die sich das leisten können und die das drohende Verschwinden von W&F mitverhindern wollen, um Unterstützung bitten. Selbstverständlich kann jede und jeder für sich – unabhängig vom FIfF – spenden oder die Zeitschrift abonnieren für momentan 35,- Euro pro Jahr oder über eine Fördermitgliedschaft ab 60,- Euro. Alternativ möchte ich eine FIfF-Aktion zur Unterstützung von W&F anregen und vorschlagen, dass alle, die mögen, ihre Spende oder ihren Antrag auf Fördermitgliedschaft mit dem Vermerk „FIfF4W&F“ versehen. Ein Antragsformular findet sich auf Seite 27. Spenden bitte auf das Konto der Informationsstelle Wissenschaft und Frieden (Sparkasse Köln-Bonn, IBAN: DE22 3705 0198 0048 0009 54, BIC: COLSDE33).

Liebe Leserinnen und Leser,
liebe UnterstützerInnen von W&F,

Marburg und Köln im März 2020

es ist schon fast ein geflügeltes Wort: Wenn man will, dass etwas bleibt, muss man es verändern. Unsere Zeitschrift »Wissenschaft und Frieden« (anfangs »Informationsdienst Wissenschaft und Frieden«) gibt es seit über 35 Jahren. Als friedenspolitisch engagierte, interdisziplinäre Zeitschrift hat sie sich bis heute behaupten können und verfügt über eine vergleichsweise stabile LeserInnenschaft. W&F transportiert wissenschaftliche Friedensforschung in die breite Öffentlichkeit in Medien und Politik. Aber das medienpolitische Umfeld hat sich stark verändert, und es ändert sich weiter. Vor allem jüngere Generationen haben andere Lesegewohnheiten entwickelt und sind weniger als ehedem bereit, sich auf das Abonnement einer Zeitschrift festzulegen. Auch im akademischen Bereich wird vermehrt mit Quellen aus dem Internet gearbeitet. Dem wollen wir uns mit »Wissenschaft und Frieden« nicht verschließen.

Wir werben für »Wissenschaft und Frieden«, weil wir von der Qualität unseres Produkts überzeugt sind: W&F nimmt als multidisziplinäre Zeitschrift, angesiedelt an der Nahtstelle zwischen Politik, Friedenswissenschaft und Gesellschaft, einen singulären Platz ein. Dies auch, weil W&F aufgrund der über lange Jahre gewachsenen ästhetischen Ausgestaltung sich als vierteljährliches Druckerzeugnis deutlich von der schnelllebigen Internet-Welt abhebt.

All dies heißt für uns, künftig Bewährtes mit Neuem zu verbinden: Die vierteljährliche Print-Ausgabe, wir haben in den vergangenen Wochen vielfältige entsprechende Rückmeldungen erhalten, wird weiter in der gewohnten Qualität erscheinen, zugleich wird aber die gesamte Internet-Präsenz neu aufgesetzt und gestärkt. Wir wollen die W&F-Webseite attraktiver und auch für mobile Geräte nutzbar machen und uns aktiver in den sozialen Medien vernetzen. Dies ist eine große Herausforderung, die mit personellen und strukturellen Veränderungen verbunden sein wird. Wir hoffen damit zugleich auf eine größere Verbreitung der Inhalte unserer Zeitschrift, um die es uns allen im HerausgeberInnenkreis, in der Redaktion und in der AutorInnenschaft letztlich ja geht.

Allein für eine solche Umstellung wird eine beträchtliche Summe Geldes benötigt. Zudem: Die Herstellungskosten der Druckausgabe sind stetig gestiegen, die Abo-Einnahmen decken diese seit Langem nicht mehr. Der tiefgreifende Umbauprozess erhöht auch die Ansprüche an die Arbeit der verantwortlichen Redaktionsstelle. Diese soll zukünftig angemessener finanziell ausgestattet werden. Auch das sind wir den Idealen unseres Zeitschriftenprojekts schuldig.

Die Antwort auf diese Herausforderung scheint einfach und ist es doch wiederum nicht: Neben dem Ausschöpfen aller Kostenersparnisse, dem Bemühen um Projektförderung und einem noch intensiveren ehrenamtlichen Engagement seitens des Vorstands und der Redaktion müssen auch die regelmäßigen Einnahmen wachsen. Dies kann nur durch eine Erhöhung der Abo-Beiträge und des Spendenaufkommens sowie die Einwerbung von mehr Fördermitgliedschaften im Trägerverein der Zeitschrift, der Informationsstelle Wissenschaft und Frieden, gewährleistet werden.

Wir bitten Sie daher um weitere Unterstützung unserer Zeitschrift und um Ihre Mithilfe beim Einwerben von neuen InteressentInnen und Fördernden.

Paul Schäfer, Mitglied der Redaktion
Johannes M. Becker, PD Dr.,
stellvertretender Vorsitzender des Vorstandes

Zur Kontaktaufnahme: *jbecker@staff.uni-marburg.de*

Wissenschaft & Frieden 2/2020 „Frieden begreifen“

Im öffentlichen Diskurs kommt das Wort *Frieden* kaum noch vor, vielmehr ist *Sicherheit* das Codewort, wenn über aktuelle Krisen und Konflikte gesprochen und verhandelt wird. W&F 2/2020 *Frieden begreifen*, unternimmt den Versuch einer Verständigung darüber, was Frieden eigentlich bedeutet, wie sich *Frieden* von *Sicherheit* unterscheidet und welche Orientierungspunkte ein solch umfassenderes Konzept für praktisch-politisches Handeln bieten könnte. Damit soll auch der Weg geöffnet werden, um über alternative Lösungsansätze in Gewaltkonflikten nachzudenken.

Es schreiben:

- *Thomas Nielebock:* Wissen, wovon wir reden – Zum Begriff des Friedens
- *Christoph Weller:* Frieden ist keine Lösung – Ein bescheidener Friedensbegriff für eine praxisorientierte Konfliktforschung
- *Claudia Kemper:* Streit um den Frieden – Die alte Bundesrepublik zwischen Krieg und Frieden
- *Theresa Bachmann:* Gewalt trotz „Frieden“ – Status quo des liberalen Friedens in Lateinamerika
- *Dorothea Hamilton* und *Matthias Grenz:* Der Frieden in Kolumbien „… ist nicht der Frieden, den wir wollen“
- *Melanie Hussak:* Lebensweltliche Frieden – Der Ritt der „Dakota 38+2“
- *Gabriella Hornung:* Interreligiöser Dialog – Friedens- und Konfliktkonzepte in Indonesien und Südkorea

Außerhalb des Schwerpunkts stellt Jürgen Scheffran Überlegungen an zu *Kollaps und Transformation – Die Corona-Krise und die Grenzen des Anthropozäns*, Herbert Wulf fragt *Ist die Denuklearisierung Koreas noch möglich?* und Otfried Nassauer untersucht *Kleine Atomsprengköpfe auf großen U-Boot-Raketen* und das damit wachsende Risiko eines Atomkrieges. Andreas Zumach schrieb den Gastkommentar zu 75 Jahren UN-Charta, und die kommentierte Presseschau spießt die Diskussion um einen neuen Atombomber für Deutschland auf.

Kampfdrohnen und Killerroboter als Mittel zur Förderung von Frieden und Gerechtigkeit? Dieses Verständnis muten SicherheitspolitikerInnen der interessierten Öffentlichkeit zu, wenn sie die Ausrüstung des Militärs mit Kampfdrohnen befürworten. Die kriegsethische Problemlage hat sich mit der Entwicklung, Verbreitung und Verwendung der militärischen Drohnentechnologie, zu der in absehbarer Zeit auch Killerroboter gehören könnten, grundlegend verändert. Damit stellt sich die Frage nach der ethischen Vertretbarkeit von militärischer Gewalt grundlegend neu. W&F-Dossier 89 *Mit Kampfdrohnen und Killerrobotern – für gerechten Frieden?* benennt das Problem und bezieht Stellung dazu.

Wissenschaft & Frieden, 2/2020: „Frieden begreifen“. 9,00 € Inland, EU plus 3,00 € Porto (Bitte um Vorkasse: Sparkasse KölnBonn, DE86 3705 0198 0048 0007 72, SWIFT-BIC COLSDE33XXX)

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F c/o BdWi-Service, Gisselberger Str. 7, 35037 Marburg, E-Mail: *vertrieb@wissenschaft-und-frieden.de*, *www.wissenschaft-und-frieden.de*

Wissenschaft und Frieden ist Trägerin des Göttinger Friedenspreises 2018

Informationsstelle Wissenschaft und Frieden
Beringstr. 14
53155 Bonn

Fördermitglied werden – die Zukunft von »Wissenschaft und Frieden« sichern!

Mit Ihrer Fördermitgliedschaft bei der Informationsstelle Wissenschaft und Frieden (IWIF) e. V. und Ihrem Förderbeitrag von mindestens 60 Euro im Jahr unterstützen Sie W&F. Die IWIF ist die Trägerorganisation von W&F. Als Fördermitglied erhalten Sie die gedruckte Ausgabe von W&F und alle Dossiers sowie auf Wunsch auch die digitale Ausgabe. Sollten Sie W&F bereits abonniert haben, wird dieses Abonnement automatisch ausgesetzt. Die Informationsstelle Wissenschaft und Frieden ist seit 1978 als gemeinnützig anerkannt. Für Förderbeiträge wie auch Spenden erhalten Sie im Januar des Folgejahres eine steuerlich abzugsfähige Spendenbescheinigung.

Ich möchte Fördermitglied der IWIF e. V. werden mit einem Jahresbeitrag von _____ €.

_____

Name, Vorname, E-Mail-Adresse (falls Sie W&F als ePub/PDF erhalten möchten), Zusatz FIfF4W&F (falls gewünscht)

_____

Anschrift

SEPA-Bankeinzug

Zahlungsempfänger: Informationsstelle Wissenschaft und Frieden e. V. (IWIF), Beringstraße 14, 53155 Bonn, Gläubiger-ID: DE75ZZZ00000726120

Ich ermächtige die IWIF e. V., ab sofort Zahlungen von meinem nachfolgend genannten Konto mittels Lastschrift einzulösen. Der erste Einzug erfolgt für den laufenden Jahresbeitrag innerhalb der nächsten vier Wochen. Das Mandat gilt anschließend wiederkehrend einmal jährlich zum 15. März des jeweiligen Jahres. Die Mandatsreferenz wird separat mitgeteilt.

Hinweis: Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen.

_____

Name des Kontoinhabers/der Kontoinhaberin

_____

Straße und Hausnummer

_____

Postleitzahl und Ort

_____ _____

IBAN BIC

_____

Kreditinstitut

_____

Datum und Unterschrift

Freie Ärzteschaft e. V. (CC BY-SA)

Walter Schmidt

Gesundheitswesen im Datenrausch

Editorial zum Schwerpunkt

Seit mehr als 20 Jahren verfolgt die Bundesregierung – völlig unbeeinflusst von der unterschiedlich geprägten parteipolitischen Zusammensetzung der jeweiligen Regierungskoalition – einen Kurs der Digitalisierung und Technisierung des öffentlichen Gesundheitswesens, mittlerweile häufig auch *Gesundheitswirtschaft* genannt.

Begleitet von interessengeleiteten Initiativen, Unternehmen und Verbänden aus dem Bereich der IT- und der Pharma-Industrie, der gesetzlichen Krankenkassen sowie der universitären und der privatwirtschaftlichen Forschung wird damit der Versuch unternommen, vorgeblich die Kosten im Gesundheitswesen zu reduzieren. Tatsächlich werden aber neoliberale und privatwirtschaftlich nutzbare Tendenzen im Gesundheitswesen verstärkt und zugleich die in Krankenhäusern und Arztpraxen anfallenden individuellen Gesundheits- und Behandlungsdaten einer Zweit- und Dritt-Nutzung zugeführt.

Insbesondere seit dem Amtsantritt des derzeitigen Bundesgesundheitsministers Jens Spahn (CDU) hat der *Digitalisierungszug* im Gesundheitswesen deutlich Fahrt aufgenommen. Nahezu im Monatstakt kommen aus dem Hause Spahn neue Gesetzentwürfe. Dies hat sich auch in der derzeit alles beherrschenden Corona-Pandemie nicht verändert, wie Mitte Mai 2020 das *Zweite Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite* deutlich machte.

Da die Europäische Datenschutz-Grundverordnung (DSGVO) eine durchaus wirksame Sperre bei der ungebremsten Nutzung von Gesundheits- und Behandlungsdaten darstellt, verwenden die bereits genannten Vereinigungen aus Industrie, Krankenkassen und Forschung einige Mühe darauf, die Grundsätze der informationellen Selbstbestimmung im Gesundheitswesen aufzuweichen. „Vom Datenschutz zum Datenschatz“ soll der Weg führen. Auch mit dem sogenannten *Dateneigentum* wird versucht, Schneisen für die wirtschaftliche Nutzung der anfallenden Daten zu schlagen.

Von Beginn an waren die Digitalisierung und Technisierung des öffentlichen Gesundheitswesens auch Gegenstand der Kritik, sowohl von gesetzlich versicherten Menschen, von ÄrztInnen und ihren Verbänden sowie von DatenschützerInnen, IT-Fachleuten und NetzpolitikerInnen. Dieser Widerstand ist nie verstummt. Er war nie so stark, dass er die Entwicklungsrichtung im Gesundheitswesen grundsätzlich verändern konnte. Aber er war stark genug, um Auswüchse zu verhindern und übergriffiges Verhalten zu begrenzen. Dies ist auch heute noch der Fall.

In fünf Aufsätzen beschäftigen sich eine Autorin und vier Autoren mit unterschiedlichen Aspekten der derzeitigen Auseinandersetzung um die Digitalisierung des Gesundheitswesens:

Sylvia Johnigk geht der Frage nach, ob In Deutschland eine radikale Transformation des Gesundheitswesens stattfindet, die grundsätzlich das Ziel verfolgt, Gesundheitsdaten einer besseren Verwertbarkeit durch Forschung und Wirtschaft zuzuführen.

Prof. Dr. **Gerd Antes** übt Kritik daran, dass „die Medizin im Datenrausch“ sei, bei Big Data im Gesundheitswesen aber eine Bewertung von Nutzen – Risiko – Kosten der Digitalisierung fehle.

Prof. Dr. **Wulf Dietrich** erörtert, wie mit dem am 1. Januar 2020 in Kraft getretenen *Implantate-Register-Gesetz* der Datenschutz ausgehebelt wird.

Dr. **Thilo Weichert** setzt sich mit dem *Digitale-Versorgung-Gesetz* auseinander, das Ende 2019 beschlossen wurde und mit dem unter dem Stichwort *Datentransparenz* auf pseudonymer Basis eine bevölkerungsweite Datenbank mit Gesundheitsdaten u. a. für Forschungszwecke geschaffen wird.

Jan Kuhlmann informiert über die Protestbewegung gegen die Telematikinfrastruktur

Walter Schmidt

Walter Schmidt (Frankfurt am Main) ist Mitglied der Bürgerrechtsgruppe *dieDatenschützer Rhein Main* (https://ddrm.de/), 15. Mai 2020

Sylvia Johnigk

Informationssicherheit und Datenschutz bleiben auf der Strecke bei der digitalen Transformation des Gesundheitswesens

In Deutschland findet eine radikale Transformation des Gesundheitswesens statt, die grundsätzlich das Ziel verfolgt, Gesundheitsdaten einer besseren Verwertbarkeit durch Forschung und Wirtschaft zuzuführen.

Gesundheitsdaten von gesetzlich Versicherten werden seit 2019 staatlich angeordnet auf zentralen Servern – bei einem kommerziellen Dienstleister – gespeichert und verarbeitet.[1] Alle Gesundheitsdaten sollen für die Forschung – staatlich/kommerziell – „frei" zugänglich sein. Mit der Digitalisierung des Gesundheitswesens und insbesondere der Einführung der Telematik Infrastruktur kommt es zu einer Umwidmung der Daten. Gesundheitsdaten werden zu Sozialdaten, wenn die Daten von einer staatlichen Stelle, gemäß § 35 SGB I, § 67 ff SGB X und § 271 SGB X durch staatliche Anforderungen abgerufen bzw. weiterverarbeitet werden sollen. Nach § 67c Sozialgesetzbuch (SGB) X dürfen Gesundheitsdaten (genauer Sozialdaten) zu Forschungszwecken auch ohne weitere Einwilligung der Versicherten ohne Anonymisierung[2] verwendet werden.

Das Wertschöpfungspotential, das in den Gesundheitsdaten liegt, ist verglichen mit anderen Daten sehr hoch. Gesundheitsdaten sind 10-mal soviel wert wie Kreditdaten.[3] Die Schätzungen bei dem Wert einer individuellen Patientenakte gehen von durchschnittlich 60 bis 150 € aus. Informationen über unveränderliche Gesundheitsdaten, wie genetische Defekte, sind noch viel wertvoller. Laut der NZZ hat *Gentech*, eine US-Tochter der *Roche-Group*, 2015 für 60 Mio US$ 3000 Datensätze aus einer Gendatenbank des App-Herstellers *23andMe* gekauft.[4]

Berücksichtigt man, dass zukünftig die Gesundheitsdaten von 74 Millionen gesetzlich Krankenversicherten auf der Telematik-Infrastruktur (TI) zentral gespeichert und verarbeitet werden sollen und legt 60 € (also einen Wert im unteren Bereich) als Wert für eine Patientenakte fest, so läge der Minimalwert der Rohdaten bei 4,4 Mrd €. Über diese Summe kann man aktuell keine Cyberversicherung abschließen.

Für kritische Infrastrukturen gilt in Deutschland seit 2015 das IT-Sicherheitsgesetz. Krankenhäuser zählen zu den kritischen Infrastrukturen. Sie müssen in ihren wichtigen Basisprozessen, insbesondere für die Versorgung der Patienten, zusätzlich zur EU-DSGVO und dem § 203 StGB die strengen Auflagen des IT-Sicherheitsgesetzes erfüllen. Das gleiche gilt für die IT-Dienstleister, die für die Betreiber kritischer Infrastrukturen Dienstleistungen in diesen Prozessen anbieten. Sicherheitstechnisch bedenklich wurde gesetzlich geregelt, dass die Telematik-Infrastruktur und die *gematik* von den Anforderungen des § 8a BSI-Gesetzes befreit sind.[5] Zusammen mit der Umwidmung von Gesundheitsdaten in Sozialdaten und somit der Vorrangigkeit des SGB, ergeben sich für die TI geringere Sicherheitsanforderungen als für Krankenhäuser oder Ärzte. Diese Entscheidung ist aus Sicherheitssicht ein Skandal, da es völlig uneinsichtig ist, Krankenhäuser als kritische Infrastruktur einzustufen und den verpflichtend zu nutzenden IT-Dienstleister nicht. Wenn der IT-Dienstleister auf Grund von Sicherheitsproblemen die Daten nicht zur Verfügung stellen kann, schränkt es die Arbeit aller Krankenhäuser und Ärzte, die gesetzlich Versicherter behandeln, erheblich ein.

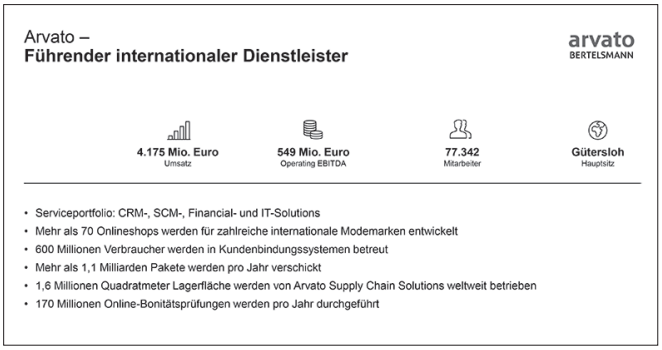
Telematik-Infrastruktur

Die Telematik-Infrastruktur soll Ärzte, Zahnärzte, Apotheken, Krankenhäuser, Krankenkassen und andere Gesundheitsdienste wie z. B. Psychotherapeuten miteinander vernetzen. Die Daten werden zentralisiert verarbeitet. Ziel ist, diese Daten jederzeit demjenigen zur Verfügung zu stellen, der sie benötigt und berechtigt ist, sie zu verwenden.

Als erste Anwendungen wurde das Versicherten-Stammdatenmanagement verpflichtend eingeführt. Weitere Anwendungen wie das Notfallmanagement sollen auf freiwilliger Basis folgen. Es steht aber zu befürchten, dass, wie bereits mehrfach in der Vergangenheit bei ähnlichen Vorgängen geschehen, diese Freiwilligkeit in einen Zwang geändert wird.

Bertelsmann als IT-Dienstleister

Arvato, ein Unternehmensteil der *Bertelsmann SE & CO KGaA*, ist der Betreiber der Telematik-Infrastruktur. Bertelsmann besitzt eine Reihe von IT-Unternehmen, wie zum Beispiel *AZ Direkt GmbH* und *Arvato Distribution GmbH*. Abgesehen davon, dass Bertelsmann bereits im digitalen Pharmahandel tätig ist, verdient Bertelsmann auch Geld mit Adresshandel, Scoring und Profiling, insbesondere auch Kreditbewertung (*Infoscore*) und Meinungsumfragen.



Zahlen aus der Unternehmenspräsentation von Bertelsmann, Stand April 2020, Quelle: https://www.bertelsmann.de/news-und-media

Mit der Telematik-Infrastruktur hat Bertelsmann – auf Grund des hohen Wertschöpfungspotentials – in Zukunft die Möglichkeit ein wirtschaftlich kräftiges Standbein aufzubauen.

Bertelsmann-Informationssicherheit und -Datenschutz

Verschiedenste Bertelsmann-IT-Unternehmen sind dadurch aufgefallen, dass sie immer wieder in Datenschutzskandale verwickelt waren:

2012 berichtete *NDR Info*[6], dass einer Frau verweigert wurde, eine Versandhauslieferung auf Rechnung zu begleichen, da eine schlechte Bewertung durch *Arvato Infoscore* vorlag. Obwohl Arvato für die Bewertung der Zahlungsfähigkeit der Frau veraltete soziodemografische Daten verwendete und keinerlei negative Bewertungen von Dritten vorlagen, wurde trotzdem eine schlechte Bewertung abgegeben. Eine Analyse durch den baden-württembergischen Landesdatenschutzbeauftragten ergab, dass Arvato Infoscore mehrfach schlechte Bewertungen für Personen abgeben hat, obwohl es keine negativen Daten gab und nur veraltete Adress-Daten vorlagen.[7]

2015 hat der NDR aufgedeckt, dass Arvato Infoscore Bonitätsauskünfte an nicht berechtigte Personen herausgegeben hat, da sie auf eine Prüfung der Ausweisdokumente verzichtet hatte. Wenn man wissen wollte, ob eine Person eine gute oder schlechte Bewertung hatte, konnte man dies bequem über eine Web-Anwendung erfahren.[8]

2018 gründeten zwei Volontärinnen des *MDR* eine Scheinfirma. Als vermeintliche Unternehmensberatung nahmen sie Kontakt zu verschiedenen Scoring-Firmen auf. Die Bertelsmann-Tochter *AZ Direct* wollte sich das Geschäft nicht entgehen lassen. Der MDR übermittelte eine Liste mit 153 Personendaten mit der Anforderung, diese um aussagekräftige Persönlichkeitsmerkmale zu ergänzen. AZ Direct fertigte daraufhin für die Personen ein Profil mit 30 zusätzlichen Persönlichkeitsmerkmalen an. Zudem hatte AZ Direkt der Unternehmensberatung auch zugesichert, dass sie datenschutzrechtlich geschützte Informationen in der Zielgruppe identifizieren könnten, zum Beispiel die sexuelle Orientierung oder die psychische Stabilität. AZ Direct räumte im Anschluss keinerlei Versäumnisse bei der fehlenden Überprüfung der Scheinfirma oder Fehlverhalten hinsichtlich datenschutzrechtlich bedenklicher Informationen ein.[9]

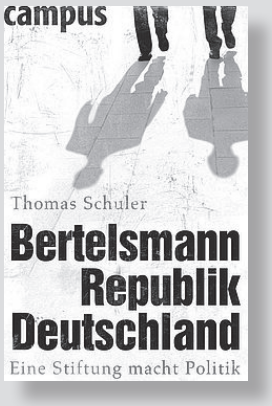
Bertelsmann hat wiederholt gezeigt, dass sie es mit dem Datenschutz, der Authentizität und der Integrität von Daten nicht so genau nehmen. Ebenso wenig hält sich Bertelsmann an die Zweckbindung und lässt unerlaubt Daten zwischen verschieden Tochtergesellschaften fließen. 2016 nutzte Arvato Infoscore Informationen, die sie aus ihren Inkasso-Dienstleistungen für die Deutsche Bahn bekam. Zu spät gezahlte oder angemahnte Tickets oder erkannte Schwarzfahrten wirkten sich negativ auf die Kreditbewertung aus.[10] Das Wissen aus dem Inkassogeschäft hätte nie gesetzeskonform für die Kreditbewertung genutzt werden dürfen.

Bertelsmann betreibt Lobbyismus für die Datensouveränität[11], die vereinfacht gesagt dazu führt, dass jede/r sich selbst um den Schutz ihrer/seiner Daten kümmern muss. Trotz wiederholten Verstößen gegen geltendes Recht und mangelnder Einsicht in eigene Fehler wurde der Vertrag zwischen der Gematik und Arvato verlängert.[12] Das ist umso problematischer, als ein Wechsel zu einem anderen Provider immer schwieriger wird, je länger die Telematik-Infrastruktur von ein und demselben Provider betrieben wird, je mehr Anwendungen betrieben und je mehr Daten verarbeitet werden. Dabei hat gerade der Fall mit der Bahn gezeigt, dass Arvato keine Skrupel hat, Daten aus einem anderen Geschäftszweig für die Kreditbewertung herzunehmen. Was das für die Gesundheitsdaten bedeuten könnte, möchte man sich lieber nicht ausmalen.

Die Bertelsmann-Stiftung als strategischer Partner

Passend zur zukünftigen *Cash Cow* Arvato-Telematik-Infrastruktur veröffentlicht die Bertelsmann-Stiftung immer wieder neue Studien wie *Der digitale Patient*[13] und untermauert damit die Gesamtstrategie des Bertelsmann-Konzerns, im E-Gesundheitswesen kräftig partizipieren zu wollen. In seinem Buch *Bertelsmann Republik Deutschland* hat der Journalist Thomas Schuler transparent gemacht, wie die Stiftung aktiv Gesetzesentwürfe und Reformen im Sinne der Unternehmensinteressen lenkt. Die Bertelsmann-Stiftung hat sich für ein Outsourcing der öffentlichen Verwaltung stark gemacht. Gleichzeitig hatte das Bertelsmann-Subunternehmen Arvato genau dafür maßgeschneiderte Lösungen angeboten. Gegen das Buch von Thomas Schuler ging die Bertelsmann-Stiftung noch am Tage der Veröffentlichung vor.[14] Sie bestritt einen Zusammenhang zwischen den Studien und den anderen Geschäftsbereichen vehement. Bertelsmann betonte ausdrücklich, dass ihre Studien der Stiftung völlig unabhängig von Geschäftsinteressen seien.

Nach der Veröffentlichung des Buchs stellte sich heraus, dass Arvato bei dem Versuch gescheitert ist, die Stadt Würzburg zu digitalisieren.[15] Arvato konnte seine Versprechen nicht einhalten. Nachdem die Stadt den 10-Jahresvertrag vorzeitig wegen Nichterfüllung gekündigt hatte, wollte Arvato auch noch Schadensersatz wegen der vorzeitigen Kündigung haben. Arvato selbst betonte, dass das Projekt erfolgreich vorzeitig nach vier Jahren beendet werden konnte, da die Stadt aufgrund der verbesserten Prozesse nun selbstständig in der Lage sei, das Projekt fortzuführen.[16]



Thomas Schuler
Bertelsmann Republik Deutschland,
Eine Stiftung macht Politik
Campus Verlag, Frankfurt
E-Book, 304 Seiten
Preis: 9,99 Euro
ISBN: ISBN 9783593408323

Die Rolle der gematik GmbH

Die *gematik GmbH* (Gesellschaft für Telematik-Anwendungen der Gesundheitskarte mbH) wurde im Januar 2005 von den Spitzenorganisationen des deutschen Gesundheitswesens gegründet.

Die gematik GmbH gehört seit 2019 zu 51 % dem Bund bzw. dem Bundesministerium für Gesundheit, zu 24,5 % dem GKV-Spitzenverband (Bundesweiter Verband der gesetzlichen Krankenkassen[17]) und zu 24,5 % der Spitzenorganisationen der Leistungserbringer. Basis dieser Änderung war das im Mai 2019 in Kraft getretene Terminservice- und Versorgungsgesetz.[18] Jens Spahn wollte mit diesem Gesetz den jahrelangen Zwist zwischen dem GKV und den Spitzenorganisationen der Leistungserbringer beenden, und kann durch die absolute Mehrheit zukünftig Entscheidungen allein und ohne Zustimmung der anderen Anteilshaber fällen.

Der Zweck der Gesellschaft ist es, gemäß dem gesetzlichem Auftrag, die Einführung, Pflege und Weiterentwicklung der elektronischen Gesundheitskarte (eGK) und der Telematik-Infrastruktur in Deutschland voranzutreiben, zu koordinieren und die Interoperabilität der beteiligten Komponenten sicherzustellen.

Umgang mit Informationssicherheit und Datenschutz bei der gematik GmbH

Am 20. November 2019 wurde von der Gematik ein neues *White Paper* zum Thema Datenschutz und Informationssicherheit[19] herausgeben. Sie selbst rühmt ihre Leistung in diesem Bereich:

> *„Bereits im Entwurfsstadium werden Datenschutz und Informationssicherheit berücksichtigt, sowohl bei der Erstellung von technischen Spezifikationen als auch bei der Entwicklung von Anwendungen, Komponenten und Diensten der Telematikinfrastruktur. Dies geschieht in enger Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die erarbeiteten Konzepte für eine Anwendung, eine Komponente bzw. einen Dienst der Telematik-Infrastruktur werden sodann von datenschutzrechtlichen Aufsichtsbehörden oder Sicherheitsprüfstellen geprüft und bewertet. Die gematik veröffentlicht alle technischen Vorgaben.“*

Diese Aussagen kann man als Euphemismus bezeichnen. Schon lange fordern viele Verbände von Datenschützern, Arztverbänden, Patientenvereinigungen, dass endlich geklärt wird, wer die datenschutzrechtlich verantwortliche Stelle für die Telematik-Infrastruktur ist, um dann einen Datenschutzbeauftragten zu benennen, der eine Datenschutz-Folgenabschätzung durchführt und diesen Bericht veröffentlicht. Am 12. September 2019 äußerte sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu der Frage der verantwortlichen Stelle mittels eines Tweets vom Bundesdatenschutzbeauftragten Herrn Kelber.[20,21] Sie ist der Auffassung, dass die gematik GmbH für die *TI Zone zentral* allein verantwortlich ist, für die *TI Zone dezentral* ist sie mitverantwortlich, wobei hierzu hinsichtlich des Umfangs gesetzliche Regelungen geschaffen werden müssen. Anzumerken sei in diesem Zusammenhang, dass der Bundesdatenschutzbeauftragte Herr Kelber im Beirat der gematik GmbH sitzt.[22]

Da bislang die verantwortliche Stelle nicht benannt wurde, ist nachvollziehbar, warum vor der Inbetriebnahme keinerlei datenschutzrechtliche Bewertungen durchgeführt wurden.

Unter diesem Umständen wird klarer, warum Arvato trotz vielfacher Datenschutzverfehlungen, falschen Bewertungen beim Profiling und dem Versagen in der Stadt Würzburg, zwar genügend Gründe geliefert hatte, dass sie sich wie rechtlich gefordert eigentlich nicht eignen, um der Betreiber einer zentralen Gesundheitsplattform zu sein, aber trotzdem die Verlängerung bekommen haben, um die TI für weitere acht Jahre zu betreiben. Zumindest sollte man als Auflagen für den Betreiber der TI eine Reihe von zusätzlichen Kontrollmechanismen etablieren, die sicherstellen, dass sich Datenschutz- und Informationsicherheits-Verstöße bei Bertelsmann nicht wiederholen.

Unabhängig davon sind die Sicherheitskonzepte, mit denen die Dienstleister, also auch Arvato, arbeiten sollen, bzw. die die Anforderungen an die Informationssicherheit bei den Dienstleistern spezifizieren, völlig veraltet. Das übergreifende *Sicherheitskonzept für die Telematik-Infrastruktur* ist vom 10. März 2008 (Tag des Aufrufs ist der 29. März 2020).[23] Das zeigt deutlich, dass die gematik GmbH nicht beachtet, dass man Sicherheitskonzepte jährlich überprüfen und überarbeiten muss[24], um sicher zu stellen, dass die Bedrohungen, die Risiken und die Anforderungen, Standards und Maßnahmen noch *State-of-the-Art* sind und der aktuellen allgemeinen Sicherheitslage entsprechen. Selbst nicht Informatik-affine Menschen werden bemerkt haben, dass es in den letzten 12 Jahren einen großen technologischen Fortschritt gegeben hat, der die Folgerung zulässt, dass das Sicherheitskonzept hätte überarbeitet werden müssen.

Sylvia Johnigk

Sylvia Johnigk forscht und arbeitet seit über 25 Jahren im Bereich IT-Sicherheit, seit 2009 ist sie selbständige Beraterin in Großkonzernen. Ebenfalls seit 2009 ist sie im Vorstand des FIfF e. V.

Der *Sicherheitsbericht 2018* der gematik sieht anders, aber nicht besser aus.[25] Der Bericht umfasst 10 Seiten, was schon sehr kurz ist. Zieht man Deckblatt, Einleitung/Zusammenfassung, Inhaltsverzeichnis, Ausblick, Abkürzungsverzeichnis und Impressum ab, bleiben gerade einmal 3,25 Seiten Nutzinhalt. Dabei werden oberflächlich die Themen *Koordinierendes Informationssicherheitsmanagement-System* (ISMS), *Computer Emergency Response Teams* (CERT), Notfallmanagement und Auditprogramm behandelt. Selbst für diese vier Themen sind die Ausführungen spärlich, davon abgesehen, dass es noch sehr viel mehr Themen gibt, die beim Betrieb der Telematik-Infrastruktur wichtig sind. Sogar unter Berücksichtigung, dass die TI erst seit Juli 2019 verpflichtend war, sollte man mit dem Controlling und dem Berichtswesen der Sicherheitsmaßnahmen und Sicherheitsvorfällen schon angefangen haben. Aufgrund der fehlenden Datenschutz-Folgenabschätzung und Risikoanalyse kommt nicht vor, welche Maßnahmen und Kontrollen eingeführt wurden, um sicherzustellen, dass Arvato daran gehindert wird, seinen kreativen und nicht gesetzeskonformen Umgang (wie oben dargelegt) auch mit Gesundheitsdaten nahtlos fortzuführen. Dieses Risiko ist mindestens genauso groß wie das, dass externe Hacker versuchen, TI von außen zu kompromittieren.

2019 sorgte die Nachricht für Aufsehen, dass viele der Konnektoren in Arztpraxen fehlerhaft installiert wurden.[26] Betroffen waren Arztpraxen, für die nur ein Parallelbetrieb in Frage kommt, da in diesen mehr als ein Arzt arbeitet, wobei auch Praxen für Parallelbetrieb konfiguriert wurden, in denen ein sequentieller Betrieb möglich wäre. In vielen Praxen traten für die Techniker größere technische Probleme auf, die sie lösten, indem Firewall und Virenscanner deaktiviert wurden und die Praxen offen wie ein Scheunentor im Internet erreichbar waren. Dies gematik bestritt das. Sie beharrte darauf, dass niemand nach der Installation unsicherer als vorher war und auch niemand allein gelassen wurde.[27] Dies sah der Techniker Jens Ernst anders, der den Skandal aufgedeckt hatte, und antwortete im Internet mit einer Presseerklärung deutlich.[28] Die gematik und die Befürworter der TI sehen das Versagen bei den Ärzten, die die Techniker nicht ausreichend überprüft hätten, ob sie die Konnektoren richtig installiert haben. Das kann meines Erachtens nicht die Lösung sein. Wie soll ein Mediziner beurteilen, ob der Techniker vernünftig gearbeitet hat? Der Rollout der Konnektoren hätte besser geplant werden und die Installation ausschließlich durch professionelle zertifizierte Unternehmen durchgeführt und abgenommen werden müssen. Ganz offensichtlich gab es nicht ausreichend qualifiziertes Personal. Es darf nicht das Problem der Ärzte sein, wenn man sie gesetzlich zwingt, diese Infrastruktur zu nutzen. Dieses Problem (nicht ausreichend qualifiziertes Personal um die Zeitvorgaben des Bundes einzuhalten beim Rollout der Konnektoren) hätte bei einer Risikobewertung festgestellt und von der gematik vor dem Rollout gelöst werden müssen, vor allem da die Konnektoren gesetzlich verpflichtend innerhalb eines Zeitfensters installiert werden mussten.

Als letzter Punkt sei zu bemerken, dass der Zugang der Versicherten zur TI erleichtert werden soll. Dies klingt auf dem ersten Blick erst mal gut. Versichert benötigen zukünftig, um ihre eigenen Daten einsehen zu können, weder ihre Gesundheitskarte noch einen Konnektor oder ein Kartenlesegerät, sondern nur eine App.[29] Das wiederum führt zu neuen Problemen. Die bisherige *einzige* Stärke des Konzepts der TI war, dass die Beteiligten sich mit einer starken Authentisierungsmethode anmelden mussten[30] und dass die Übertragungen verschlüsselt erfolgt. Es gibt bislang für Apps noch kein vergleichbares gleich starkes Authentisierungsverfahren, das man bei der Anmeldung an einem Server verwenden kann. Eines der einfachsten Grundsätze der Sicherheitsindustrie lautet: Die Gesamtsicherheit eines System ist so stark wie ihr schwächstes Glied. Eine Zugriffsmöglichkeit mit einer App schwächt die TI. Es scheint, dass mit einem vereinfachten Zugang zu den Daten die Akzeptanz bei den Versicherten gesteigert werden soll. Dieses Vorgehen ist grob fahrlässig, da sich die Sicherheit der Telematik-Infrastruktur massiv verschlechtert. Zudem handelt es sich bei vielen, insbesondere älteren Smartphones, um unsichere Geräte die keine Sicherheits-Updates mehr erhalten. Viele Apps bauen Datenverbindungen zu Facebook oder Google auf Es besteht die Gefahr, dass diese Apps zukünftig versuchen, die Gesundheitsdaten abzugreifen. Bleibt zu hoffen, dass Versicherte sehr schnell zu mündigen und vor allem fachkundigen Bürgern werden.

Ende 2019 deckten Sicherheitsforscher auf, dass man, ohne großartige Prüfprozesse zu durchlaufen zu müssen, die Konnektoren und gültige Zugangsberechtigungen, also spezielle Chipkarten, bequem im Internet bestellen kann und sich so mit der TI verbinden kann, obwohl man nicht zu dem berechtigten Personenkreis gehört.[31] Somit wurde gezeigt, dass sich ein eigentlich starkes technisches Authentisierungsverfahren dadurch schwächen lässt, dass man die Identitätsprüfung organisatorisch mangelhaft durchführt.

Fazit

Auf Kosten des Datenschutzes, der Informationssicherheit und der Gesundheit der Patienten wird aus ökonomischen Interessen die Digitalisierung des Gesundheitswesen vorangetrieben. Wer nicht mitläuft, wird zum hinterwäldlerischen Technikfeind erklärt. Datenschutz wird sukzessive umgangen, technische Probleme klein geredet und organisatorische Mängel scheinen nicht zu interessieren.

Anmerkungen

1 *Für (Zahn-) Ärzte und Psychotherapeuten hat der Gesetzgeber die Teilnahme am Versicherten-Stammdatenmanagement VSDM (und damit den Anschluss an die TI) bereits vor geraumer Zeit verpflichtend angeordnet. https://www.iww.de/aaa/recht/telematikinfrastruktur-ti-anschluss-wem-droht-die-honorarkuerzung-f122727*

2 *§ 67c Abs (5) Für Zwecke der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich erhobene oder gespeicherte Sozialdaten dürfen von den in § 35 des Ersten Buches genannten Stellen nur für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich oder der Planung im Sozialleistungsbereich verändert oder genutzt werden. Die Sozialdaten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Planungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Planungszweck dies erfordert.*

3 *https://www.althammer-kill.de/news-detail/gesundheitsdaten-sind-*

wertvoller-als-finanzdaten
4 https://www.nzz.ch/wirtschaft/gewisse-gesundheitsdaten-sind-goldwert-1.18546205
5 https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_8aBSIG_allgemein/faq_bsi_8a_allgemein_node.html
6 https://www.ndr.de/der_ndr/presse/mitteilungen/Datenleck-bei-grosser-Auskunftei-Kritik-an-Bertelsmann-Tochterfirma-Infoscore,pressemeldungndr15596.html
7 https://www.heise.de/newsticker/meldung/Bericht-Infoscore-nutzt-veraltete-Daten-bei-Bonitaetsberechnung-1545563.html
8 https://www.heise.de/newsticker/meldung/NDR-Mangelhafter-Datenschutz-bei-Bertelsmann-Auskunftei-Infoscore-2583029.html
9 https://www.mdr.de/datenspuren/datenspuren-162.html
10 https://www.zeit.de/digital/datenschutz/2016-05/bahn-kundendaten-infoscore-schwarzfahren
11 https://www.bertelsmann-stiftung.de/de/unsere-projekte/teilhabe-in-einer-digitalisierten-welt/projektnachrichten/datensouveraenitaet-in-zeiten-von-big-data/
12 https://www.gematik.de/news/news/gematik-erteilt-zuschlag-im-vergabeverfahren-zur-zentralen-telematikinfrastruktur/
13 https://www.bertelsmann-stiftung.de/de/unsere-projekte/der-digitale-patient/
14 https://www.deutschlandfunk.de/nur-im-eigenen-interesse.1310.de.html?dram:article_id=194162
15 https://www.mainpost.de/regional/wuerzburg/Flop-mit-Arvato-kostet-Stadt-ueber-eine-halbe-Million;art735,7710299
16 https://www.kommune21.de/meldung_11581
17 https://www.gkv-spitzenverband.de/
18 https://www.bundesgesundheitsministerium.de/terminservice-und-versorgungsgesetz.html
19 https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_Whitepaper_Datenschutz_und_Informationssicherheit.pdf
20 Tweet von Herrn Kelber https://twitter.com/ulrichkelber/status/1176079363340718081
21 Link aus dem Tweet von Herrn Kelber https://t.co/G42Saj437i
22 https://www.gematik.de/ueber-uns/unternehmensstruktur/
23 https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Basis-Rollout/Datenschutz_und_Datensicherheit/gematik_DS_Sicherheitskonzept_V2_2_0.pdf
24 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/ISMS/Umsetzungshinweise_zum_Baustein_ISMS_1_Sicherheitsmanagement.html siehe ISMS 1.M11 Aufrechterhaltung der Informationssicherheit Absatz 4 „Diese Überprüfungen sollten zu festgelegten Zeitpunkten (mindestens jährlich) durchgeführt werden und können auch zwischendurch erfolgen."
25 https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/2019-01_gematik_Sicherheitsbericht_2018.pdf
26 https://www.heise.de/newsticker/meldung/Telematik-im-Gesundheitswesen-Freie-Aerzteschaft-warnt-vor-unsachgemaesser-Konnektor-Installation-4406506.html
27 https://www.aend.de/article/201216
28 https://www.happycomputer.eu/index.php/presseartikel/
29 https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_Whitepaper_Datenschutz_und_Informationssicherheit.pdf Kapitel 6.6
30 Leider bezieht sich die Aussage nur auf die Technik – siehe nächsten Absatz
31 https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt

Gerd Antes

Big Data – die Medizin im Datenrausch

Evidenz aus Studien vs. unstrukturierte Daten?

Die allgegenwärtig fehlende Bewertung von Nutzen – Risiko – Kosten der Digitalisierung ist nicht wissenschaftlich zu erklären, berichtet Prof. Dr. Gerd Antes, Freiburg. Sie wird jedoch sofort einleuchtend, wenn man erkennt, dass wir es nicht mit der Entwicklung zum Vorteil der Patienten zu tun haben, sondern mit Realisierung einer Ideologie, deren Ziele und Sinn nicht hinterfragt werden können. Ärzteschaft, Gesundheitsprofession und Patienten sind gefordert, das Menschliche in der Medizin zu erhalten oder aber bewusst darauf zu verzichten, sich jedoch nicht von der Technik überrollen zu lassen [1].

Die Welt scheint nur noch ein Ziel zu haben: Digitalisierung! Es gibt keine Entwicklungen mehr, für die nicht phantastische Fortschritte angekündigt werden, wenn die Digitalisierung nur konsequent angegangen wird. Selbst eine oberflächliche Betrachtung lässt jedoch schnell Ernüchterung einkehren. Für eine solch alles erfassende, technikgetriebene Umwälzung sollte man eine auf Hochtouren laufende Technikfolgenabschätzung erwarten. Weit gefehlt, man findet diese überhaupt nicht oder von den dort üblichen Dimensionen:

- Nutzen
- Risiko/Schaden
- Kosten

nur den Nutzen. Mögliches Risiko und Schäden, wie zum Beispiel Fehlentwicklungen, werden nicht thematisiert, genauso wenig die Kosten. Wo nur Nutzen existiert, scheinen alle Kosten gerechtfertigt.

Big Data: Zukunftsversprechen auf einem brüchigen Fundament

Seit circa 15 Jahren wird die Vision entwickelt und über vielfache Kanäle verbreitet, dass der kommende Überfluss an Daten uns eine bessere Welt durch unbeschränkte Erkenntnis eröffnet. Für den gesunden Menschenverstand erscheint diese Aussage so selbstverständlich, dass sie nicht hinterfragt werden muss. In einem einflussreichen Artikel wurde diese eingängige, jedoch naive Einschätzung vor circa 10 Jahren wissenschaftlich formuliert, indem das Ende der Theorie verkündet wurde: Die Datensintflut macht die wissenschaftliche Methode überflüssig [2]. Die Aus-

sagen in diesem Artikel führten, da sie mit den Grundlagen des Wissenschaftssystems nicht vereinbar waren, in eine neue Wissenschaftswelt und verfestigten diese durch regelmäßige, unkritische Wiederholung.

Während die empirische Forschung der alten Erkenntniswelt in den letzten Jahrzehnten durch ein stetes Ringen um Qualität charakterisiert war, erscheint das in der neuen, unbeschränkten Datenwelt überflüssig. Aufwendige Qualitätssicherungsmaßnahmen werden ohne theoretisches Fundament durch unbegrenzten Datenreichtum ersetzt. Aussagen zur Ergebnisqualität sowie Forderungen zur guten wissenschaftlichen Praxis und speziell zur *Good Clinical Practice* sucht man vergebens.

Sehr ähnlich sieht es bei der Nutzung und Auswertung großer Datenbestände mit künstlicher Intelligenz (KI) aus: Statt detaillierter Methodenbeschreibungen in klassischen Auswertungen findet man jetzt oft nur den Satz „… wurde mit künstlicher Intelligenz ausgewertet …".

Fundamentale wissenschaftliche Schwachpunkte

Big Data entzieht sich der kritischen Bewertung durch eine Definition, die keine ist. Üblicherweise wird Big Data durch 3 (inzwischen auch 5) „V" charakterisiert:

- Datenmenge (Volume),
- Geschwindigkeit (Velocity) und
- unterschiedliche Beschaffenheit (Variety).

Die fehlende Quantifizierung erlaubt keine eindeutige Qualifizierung, ob ein großer Datenkörper dazu gehört oder nicht. Entsprechend groß sind die terminologische Verwirrung und der daraus folgende Begriffswirrwarr.

Zentraler Mechanismus von Big Data ist die Interpretation von „entdeckten" Korrelationen als Kausalzusammenhang. Bedingung ist, dass ausreichend – und damit unbeschränkt – Daten zugänglich sind. Diese Aussage ist falsch, wie in sehr anspruchsvollen mathematischen Arbeiten [3] dargelegt wird. Mehr Daten sind nicht äquivalent mit mehr Information, vor allem nicht mit weniger Aufwand, wie im Big-Data-Mainstream allerorten vermittelt wird. Diese kontraintuitive Aussage ist nur schwer zu veranschaulichen. Am besten so: Bei der Suche nach Zusammenhängen sind falsch positive Funde unvermeidlich. Diese können in wachsenden Datenmengen schneller zunehmen als die richtigen Funde, das heißt diese Signale gehen zunehmend in wachsendem Rauschen unter. Anschaulich formuliert heißt das, die Nadel befindet sich in einem größer werdenden Heuhaufen und der Aufwand, sie zu finden, nimmt nicht ab, sondern wächst sogar [4].

Big Data in der Medizin: Spezielle Herausforderungen

Medizin und Gesundheitsversorgung sind in dieser Entwicklung Getriebene und Treiber. Getrieben, da sie vor allem in dem von Internetriesen getriebenen Hype aufgrund der enormen Budgets ein einladendes Ziel mit neuen, großen Märkten sind. Treiber, da sowohl Patienten und Gesunde wie auch die Gesundheitsprofessionen und Institutionen sehr anfällig für die Verkündigungen von verbesserter Diagnostik und Therapie durch Big Data sind.

Die oben dargestellten Charakteristika von Big Data gelten in jeder Beziehung auch für die Medizin, in mehrfacher Hinsicht hat die Medizin darüber hinaus eine Sonderrolle. Vor allem die Missachtung von Risiken und Kosten hat hier eine Bedeutung, die sehr viel ernster genommen werden muss als in anderen fachlichen Zusammenhängen, wo auftretende Schädigungen als Verschwendung abgetan werden können. In der Medizin kann es vermeidbare Krankheit und Tod bedeuten und ist damit unvereinbar mit dem Prinzip, dass der Schutz des Patienten über allem steht.

Spezielle Ausprägungen aufgrund der Datenflut sind die Hoffnung auf immer individualisiertere Behandlungsmöglichkeiten mit automatisierten Entscheidungsprozessen. Diese Entwicklungen machen es weitgehend unmöglich, einzelne Begriffe aus Digitalisierung, künstlicher Intelligenz, Deep Learning, Big Data, personalisierter oder individualisierter Medizin isoliert zu betrachten, da sie untrennbar miteinander verbunden sind. Eine Folge davon sind verwirrte Diskussionen aufgrund nicht eindeutiger Definitionen.

Deutlich wird das beim Thema „Vertrauen in Daten" und den unvermeidlichen Entscheidungen unter Unsicherheit (uncertainty). Ebenso wie der Qualitätsbegriff ist die Betrachtung und Quantifizierung von Unsicherheit in der KI- und Big-Data-Welt weitgehend verschwunden. Dank unbegrenzter Daten wird das Bild vermittelt, dass damit Qualitätsprobleme und Unsicherheit nicht mehr thematisiert werden müssen. Das ist fachlich nicht haltbar und birgt die Gefahr von Patientengefährdung und systematischer Fehlentwicklung (mehr Daten erlauben, Fehler mit größerer Präzision zu machen).

Die Medizinsysteme sind gefordert, alle Anstrengung darauf zu verwenden, in den unter dem Schlagwort Digitalisierung laufenden Entwicklungen die Spreu vom Weizen zu trennen und wie-

Gerd Antes

Prof. Dr. rer. nat. **Gerd Antes**, Institut für Didaktik und Ausbildungsforschung in der Medizin, Klinikum der Universität München, LMU München. Gerd Antes ist Mathematiker, Biometriker und ehemaliger Direktor des Deutschen Cochrane Zentrums, ein internationales Netzwerk, das die wissenschaftlichen Grundlagen für Entscheidungen im Gesundheitssystem verbessern will.

der das in den Mittelpunkt zu stellen, was an vielen Brennpunkten nicht mehr in der ersten Reihe steht: der Patientennutzen.

Das bedeutet die konsequente Nutzung der über Jahrzehnte entwickelten Bewertungsinstrumente für diagnostische und therapeutische Verfahren. Besondere Aufmerksamkeit gebührt dabei nicht offengelegten, kommerziellen Gesundheits-Apps sowie den sogenannten Prozeduren der künstlichen Intelligenz, die weitgehend als Black Box beschrieben werden und ohne Regulierung in die Gesundheitsversorgung eindringen [5]. Ebenso gilt es, dem wissenschaftlichen Grundprinzip, an vorhandenes Wissen anzuknüpfen, wieder höchste Priorität zu geben, anstatt es unter dem Schlagwort „disruptiv" zu ignorieren und zu Sprunginnovation aufzurufen.

Referenzen

[1] Thielscher C, Antes G (2019) Der Arzt behält die Deutungshoheit trotz KI. Dtsch. Arztebl. 2019; 116: A 18/B 18/C 18.
Im Internet: www.aerzteblatt.de/archiv/204288/ Der Arzt behält die Deutungshoheit trotz KI

[2] Anderson C (2008) The End of Theory: The Data Deluge Makes the Scientific Method Obsolete.
Im Internet: https://www.wired.com/2008/06/pb-theory/

[3] Meng XL, Xie X Forthcoming. I Got More Data, My Model Is More Refined, but My Estimator Is Getting Worse! Am I Just Dumb? Econometric Reviews.
Im Internet: https://dash.harvard.edu/handle/1/10886849

[4] Taleb N (2013) The Big Errors of Big Data.
Im Internet: https://fs.blog/2013/02/the-big-errors-of-big-data/

[5] Leetaru K. (2019) How Data Scientists Turned Against Statistics. Im Internet: https://www.forbes.com/sites/kalevleetaru/2019/03/07/how-data-scientists-turned-against-statistics/

Dieser Beitrag ist erstmals erschienen in: Sonderdruck Current congress zum 125. Kongress der Deutschen Gesellschaft für Innere Medizin e. V., Wiesbaden 4.-7. Mai 2019, Karl Demeter Verlag. Wir danken für die freundliche Genehmigung zum Wiederabdruck.

Wulf Dietrich

Das Implantate-Register-Gesetz

... oder wie hebelt man den Datenschutz aus?

„Aber es geht! – Wir sind damit gut durchs Kabinett gekommen!" Voll Stolz präsentierte Gesundheitsminister Spahn auf dem DEMA-Kongress im April 2019 seinen Entwurf des Implantateregister-Errichtungsgesetz (EIRD)[1], mit dem er weitgehende Einschränkungen des Datenschutzes durchsetzen konnte. Gab es bei der Verabschiedung des Digitalen Versorgungsgesetzes (DVG) noch heftige Diskussionen darüber, ob die Sozialdaten der PatientInnen in großem Umfang weitergegeben und verarbeitet werden dürfen, so lief die Verabschiedung des EIRD im September diesen Jahres fast geräuschlos über die Bühne. Dabei enthält dieses Gesetz weitaus gravierendere Eingriffe in das Recht des Patienten auf personelle Selbstbestimmung als das DVG. Während im DVG die Weitergabe und Verarbeitung der so genannten Sozialdaten, also der Abrechnungsdaten, die bei den Kostenträgern anfallen und schon jetzt für epidemiologische Auswertungen herangezogen werden, intensiviert wird, sollen nach dem EIRD alle relevanten Befunde und die Anamnese der ImplantatträgerInnen weitergegeben werden – und zwar ohne Widerspruchsrecht der Betroffenen. Meldet eine Klinik einen Eingriff nicht ans Register, wird der Eingriff nicht vergütet.

Implantateregister-Errichtungsgesetz – Ein harmlos klingender Name, der suggeriert, dass hier ein durchaus sinnvolles Register medizinischer Produkte geschaffen werden soll, wie es eine EU-Richtlinie schon seit einigen Jahren fordert. Doch handelt es sich bei dem Register nicht um ein Produktregister, sondern um eine PatientInnen-Datenbank, die alle PatientInnen mit implantierten Produkten erfasst, und zwar zwangsweise. Das Register soll, so der Gesetzestext, dem Schutz der Sicherheit der PatientInnen, der Qualitätssicherung, der Marktüberwachung, sowie statistischen und wissenschaftlichen Zwecken dienen. Alle Implantattypen von Gelenkersatz, über Brustimplantate und Herzschrittmacher bis hin zu Stents sollen mit diesem Gesetz erfasst werden.

Sicher kann man über den Sinn und Unsinn von klinischen oder epidemiologischen Registern streiten (Krebsregister, Transplantationsregister, Endoprothesenregister), doch ist die Teilnahme der PatientInnen an diesen Registern meist freiwillig und die übermittelten Daten sind sehr streng begrenzt. Die Notwendigkeit eines Implantatregisters wird schon im ersten Satz der Begründung dieses Gesetzes mit dem Skandal um fehlerhafte Brustimplantate im Jahr 2010 begründet. Dabei handelte es sich bei diesem Skandal eindeutig um das Problem der CE-Zertifizierung durch den TÜV und nicht um eines der medizinischen Versorgung. Unzweifelhaft ist, dass es für Medizinprodukte, die im Körper bleiben, künftig schärfere Zulassungsverfahren geben muss, aber das hat nichts mit dem vorliegenden Gesetz zu tun.

Mit dem EIRD wird das aus den Grundrechten abgeleitete Recht auf informationelle Selbstbestimmung der PatientInnen weitgehend außer Kraft gesetzt. Jeder Patient, dem ein medizinisches Implantat eingesetzt wird, wird jetzt verpflichtet, sensiblen Gesundheitsdaten zentral einem Register in zum Teil pseudonymisierter Form zur Verfügung zu stellen. Technisch-organisatorische, klinische und zeitliche Daten zum Versorgungsprozess, wie insbesondere „Daten zur Anamnese, implantatrelevante Befunde, die Indikationen, die relevanten Voroperationen, die Größe, das Gewicht und die Befunde der Patientin oder des Patienten, das Aufnahmedatum, das Datum der Operation und das Datum der Entlassung" müssen der Registerstelle übermittelt werden (§ 16). Vom Grundsatz der im DSGVO definierten Datenminimierung ist nicht mehr die Rede. Ausdrücklich steht den

PatientInnen „kein Anspruch zu auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO oder Widerspruch nach Artikel 21 DGSVO“ zu (§26). Mit der Berufung auf Artikel 23 DSGVO wird der Datenschutz bewusst ausgehebelt. Dieser Artikel der DGSVO sieht die Beschränkung der Betroffenenrechte in schwerwiegenden Fällen wie zur Sicherstellung der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit vor. Diese Beschränkungen müssen ausführlich begründet werden (vielleicht umfasst die Begründung des EIRD deshalb fast 100 Seiten).

Wenn schon „die Verbesserung der medizinischen Versorgung mit Implantaten und langfristig der Gesundheit der Bevölkerung und kurzfristig auch der Gesundheit einzelner Patientinnen und Patienten“ solch schwerwiegenden Eingriff in die Grundrechte der PatientInnen rechtfertigt und damit der Sicherstellung der nationalen Sicherheit und der Terroristenbekämpfung gleichgestellt wird, dann ist der Datenschutz endgültig ausgehebelt. Weniger Datenschutz ist gut für die allgemeine Gesundheit der Bevölkerung – so die These. (Oder, wie Spahn schon früher feststellte: „Datenschutz ist etwas für Gesunde“.) Welche Begründung gibt es dann noch, diese Einschränkung des Datenschutzes nicht auch für Volkskrankheiten wie Diabetes, Herzinfarkt oder maligne Erkrankungen zu fordern?

Interessant ist hierbei die Begründung dieser Einschränkung der individuellen Rechte:

> *„Der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Dieses Recht ist aber nicht schrankenlos gewährleistet. Der Einzelne hat kein Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über seine Daten. Er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Informationen, auch soweit sie personenbezogen sind, stellen ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann.“* [2]

Also ist das Grundrecht auf informationelle Selbstbestimmung kein individuelles Recht, sondern ein durch die soziale Gemeinschaft determiniertes Recht, welches der Staat einschränken kann.

Diese Interpretation ist den Intentionen der DSGVO diametral entgegengesetzt. Lapidar wird die weitgehende Abschaffung des Datenschutzes begründet: „Die verpflichtende Datenübermittlung an das IRD und die Beschränkung des Rechts der betroffenen Patientinnen und Patienten auf informationelle Selbstbestimmung sind damit zur Erreichung der gesetzgeberischen Zwecke notwendig“[3] Und weil man schon einmal dabei ist, den Datenschutz auszuhöhlen, wird beschlossen, die schon in bestehenden Registern mit Zustimmung der Patienten gesammelten Daten in das neue Register ohne explizite Zustimmung zu überführen: „Für betroffene Patientinnen und Patienten komfortabler ist daher eine Datenübertragung unter Einräumung eines Widerspruchsrechts.“[4] Die explizite Zustimmung der PatientInnen zur Übertragung ihrer einmal gespendeten Daten in ein anderes Register ist nicht mehr erforderlich.

> *Heribert Prantl fasst in einem Kommentar der SZ die Kritik am EIRD treffend zusammen: „Der Datenschutz, wie ihn die Europäische Datenschutzgrundverordnung besonders für sensible Gesundheitsdaten proklamiert, wird in diesem Gesetz weitgehend abgeschafft – aus Fürsorge gegenüber dem Patienten, wie Gesundheitsminister Jens Spahn (CDU) behauptet. Der Patient wird also aus Fürsorge entmündigt … So ist aus der Datenaskese, die einst das Volkszählungsurteil forderte, eine Datenekstase geworden.“*[5]

Bewusst hat Spahn mit diesem Gesetz die Möglichkeiten der Aushöhlung des Datenschutzes ausgelotet. „Aber es geht! – Wir sind damit gut durchs Kabinett gekommen!“ Ja, es geht, man kann auch im Zeitalter der DSGVO den Datenschutz aufweichen, es muss nur gut begründet werden. Was hier an einem relativ unwesentlichem Register-Gesetz geschickt und von der Öffentlichkeit kaum bemerkt durchexerziert wurde, lässt sich analog auch in anderen Bereichen anwenden. Die Instrumente zur Untergrabung des Datenschutzes könnten als Blaupause für weitere Gesetze gelten. Wenn erst einmal die Daten der elektronischen Patientenakte zentral vorliegen, könnte man mit gleicher Begründung wie bei den Implantaten mit Hinweis auf die Bedrohung der Volksgesundheit durch Diabetes, Krebs oder Demenz und die Fürsorgepflicht des Staates auf zwangsweise Datenspende dringen. Das verabschiedete Gesetz entkräftet die Bedenken gegen Telematikinfrastruktur und zentrale Sammlung von Gesundheitsdaten keineswegs. Im Gegenteil.

Dieser Beitrag ist erstmals erschienen in: Gesundheit braucht Politik | Zeitschrift für eine soziale Medizin 4/2019, S. 13-14. Wir danken für die freundliche Genehmigung zum Nachdruck.

Anmerkungen

1 *Entwurf Implantateregister-Errichtungsgesetz (EIRD) vom 29.05.2019, Drucksache 19/10523, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/I/Implantateregister-Errichtungsgesetz_Kabinett.pdf;*

Wulf Dietrich

Prof. Dr. **Wulf Dietrich** ist Kardioanästhesist und war bis 2017 Vorsitzender des *Vereins demokratischer Ärztinnen und Ärzte (vdää)* und ist heute Mitglied des erweiterten Vorstands.

inzwischen: Gesetz zur Errichtung des Implantateregisters Deutschland und zu weiteren Änderungen des Fünften Buches Sozialgesetzbuch (Implantateregister-Errichtungsgesetz–EIRD) vom 12. Dezember 2019, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl119s2494.pdf#__bgbl__%2F%2F%5B%40attr_id%3D%27bgbl119s2494.pdf%27%5D__1582458723020*

2 ebenda, S. 36
3 ebenda, S. 38
4 ebenda, S. 88
5 Süddeutsche Zeitung, 26. Oktober 2019

Thilo Weichert

Die zentrale Speicherung von Daten der gesetzlichen Krankenversicherung

Ende 2019 wurde das Digitale-Versorgung-Gesetz *beschlossen, mit dem unter dem Stichwort* Datentransparenz *auf pseudonymer Basis eine bevölkerungsweite Datenbank mit Gesundheitsdaten u. a. für Forschungszwecke geschaffen wird, ohne dass hinreichende Vorkehrungen für einen datenschutzkonformen Umgang mit den Daten getroffen werden.*

1 Gesetzgeber beschließt Gesundheitsdatenbank

Die Empörung vieler Bürgerrechtler war und ist groß: Bundesgesundheitsminister Jens Spahn stellt ein *Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation*, abgekürzt *Digitale-Versorgung-Gesetz*, vor und zieht es durch, so dass es mit wenigen Änderungen Ende 2019 in Kraft tritt[1]: In dem Gesetz ist eine zentrale Speicherung aller Leistungsdaten von gesetzlich Krankenversicherten vorgesehen, also der Gesundheitsdaten von mehr als 70 Millionen Bürgerinnen und Bürger. Das Gespenst der zentralen Speicherung der Daten der Gesetzlichen Krankenversicherung (GKV) einschließlich der elektronischen Patientenakten, mit dem über Jahre hinweg der elektronischen Gesundheitskarte (eGK) und der Telematik-Infrastruktur (TI) das Leben und Entwickeln – zu Unrecht – schwer gemacht wurde, wird plötzlich Realität, wenn auch die Ablage der Daten nicht mit Klarnamen, sondern unter Pseudonym erfolgen soll. Das Bundesgesundheitsministerium (BMG) will mit den Daten „Datentransparenz" herstellen; die pseudonymisierten Datensätze sollen insbesondere in der Gesundheitsforschung genutzt werden können.

Konkret geht es unter der Überschrift *Datentransparenz* um eine Neufassung der §§ 303a-303f SGB V. Dieser zweite Titel des 10. Kapitels des SGB V wurde 2003 eingeführt. Unter der damaligen rot-grünen Bundesregierung sollte – mit aktiver Unterstützung von Datenschützern – eine Datengrundlage geschaffen werden für Zwecke des Risikostrukturausgleichs, aber auch für andere anonyme Auswertungszwecke. Dieses Instrument fristete über viele Jahre hinweg ein Mauerblümchendasein. Das soll sich mit dem Willen der schwarz-roten Regierung und deren Minister Spahn nun grundlegend ändern.

„Gesundheitsbank" für alle? – Foto: Manfred Antranias Zimmer

Erst kurz vor der endgültigen Beschlussfassung im Bundestag drang die Relevanz der geplanten Änderung ins öffentliche Bewusstsein. Die Kritik am Regierungsvorschlag führte dazu, dass drei Tage vor der entscheidenden Sitzung im Bundestag als Änderung beschlossen wurde, die Übermittlung durch die Krankenkassen nicht mit dem eindeutig zuordenbaren Versichertenkennzeichen vorzunehmen, sondern unter einem nicht zuordenbaren spezifischen Pseudonym. Mehr an Korrektur schien der Mehrheit nicht nötig. Eine Analyse des nun verabschiedeten Gesetzes zeigt, dass die Gesundheitsdaten der deutschen Bevölkerung künftig nicht gerade frei verfügbar sein werden, dass aber die Sicherung dieser Daten unzureichend ist.

2 Das gesetzliche Verfahren der *Datentransparenz*

Gemäß dem neuen Gesetz erfolgt eine massive Ausweitung sowohl des Datensatzes wie auch der möglichen Nutzungen. Der europäische Gesetzgeber hat in der Datenschutz-Grundverordnung (Artikel 9 Absatz 2 lit. i DSGVO) festgelegt, dass die Auswertung zentralisierter Gesundheitsdaten ausschließlich „aus Gründen des öffentlichen Interesses" zulässig ist, etwa zwecks „Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren" oder zur „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten". Auch bei einer Verwendung für wissenschaftliche Forschungszwecke nach Artikel 9 Absatz 2 lit. j DSGVO muss, wenn eine privilegierte Datennutzung erfolgen soll (Artikel 5 Absatz 1 lit. b DSGVO), ein überwiegendes öffentliches Interesse vorliegen.[2] Artikel 9 Absatz 2 lit. i, j DSGVO fordert zudem „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person". Davon ist im nun geltenden DVG nicht viel zu finden.

Zuständig für die Datentransparenz sind eine Vertrauensstelle und ein Forschungsdatenzentrum (früher: Datenaufbereitungsstelle). Die Benennung dieser „öffentlichen Stellen des Bundes" erfolgt per Rechtsverordnung durch das BMG. Sie sind räumlich, organisatorisch und personell eigenständig, d. h. auch voneinan-

der getrennt zu führen und unterliegen der Rechtsaufsicht des BMG (§ 303a Absatz 1, 2 SGB V), das also nur eine Rechtskontrolle durchführen und keine fachlichen Weisungen geben darf. Eine rechtliche Unabhängigkeit hätte man zweifellos klarer und besser ins Gesetz schreiben können.

Die Daten werden von den Krankenkassen über den Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband) zu jedem Versicherten mit einem nur kurzfristig verwendeten „Lieferpseudonym" angeliefert. Der GKV-Spitzenverband prüft die Daten auf Vollständigkeit, Plausibilität und Konsistenz und klärt offene Fragen mit der jeweiligen liefernden Krankenkasse ab und übermittelt dann die Daten incl. Alter, Geschlecht und Wohnort des Patienten, Angaben zum Versicherungsverhältnis sowie den Kosten- und Leistungsdaten nach den §§ 295, 295a, 300, 301, 301a und 302 SGB V an das Forschungsdatenzentrum ohne Lieferpseudonym mit einer Arbeitsnummer. Auch die Angaben zu den Leistungserbringern (also Ärzten, Apotheken usw.) werden vor der Übermittlung pseudonymisiert. Der GKV-Spitzenverband liefert parallel eine Liste der Lieferpseudonyme mit deren Zuordnung zu den Arbeitsnummern an die Vertrauensstelle (§ 303b SGB V).

Bisher stand für den sehr beschränkten Umfang der gesammelten pseudonymen Datensätze der Risikostrukturausgleich (§ 268 SGB V) im Vordergrund. Künftig können grundsätzlich alle Kosten- und Leistungsdaten übermittlungspflichtig gemacht werden. In einer Rechtsverordnung werden Art und Umfang der Daten (Datenfelder und Detailtiefe) bestimmt (§ 303a Absatz 4 Nr. 1 SGB V). Erfasst werden Krankenhausbehandlung (§ 301), ambulante Versorgung (§§ 295, 295a), Arzneimittel (§ 300), Heil- und Hilfsmittel incl. Digitalanwendungen (§ 302), Dienste von Hebammen (§ 301a) und anderen Leistungserbringern (etwa Physiotherapeuten, § 302). Die Ausweitung umfasst nun auch Angaben zu den Leistungserbringern.[3] Bzgl. der Angaben zum Wohnort der Patientinnen und Patienten sollen insbesondere in Großstadtgemeinden und Flächenkreisen Zuordnungen zu Lebens- und Sozialräumen möglich sein. Die Angaben zum Versichertenverhältnis können Angaben zum Versichertenstatus, Vitalstatus einschließlich des Sterbedatums der Versicherten umfassen.[4]

Die Vertrauensstelle überführt die Lieferpseudonyme in periodenübergreifende Pseudonyme, so dass „für das jeweilige Lieferpseudonym eines jeden Versicherten periodenübergreifend immer das gleiche Pseudonym erstellt wird, aus dem Pseudonym aber nicht auf das Lieferpseudonym oder die Identität des Versicherten geschlossen werden kann" (§ 303c Absatz 2). Die Vertrauensstelle übermittelt dann diese Pseudonyme mit den Arbeitsnummern dem Forschungsdatenzentrum und löscht die Lieferpseudonyme, Arbeitsnummern und übermittelten Pseudonyme (§ 303c Absatz 3 SGB). Die Generierung der Pseudonyme wird in einer Rechtsverordnung geregelt (§ 303a Absatz 4 Nr. 3).

Das Forschungsdatenzentrum hat nach § 303d Absatz 1 SGB V die Aufgabe, die angelieferten Daten zu speichern, aufzubereiten und auszuwerten. Dazu gehört die Qualitätssicherung der Daten, die Prüfung von Anträgen auf Datennutzung, das Führen eines Antragsregisters mit Informationen zu den Nutzungsberechtigten incl. Vorhaben und deren Ergebnisse und die Bereitstellung der benötigten Daten an die Nutzungsberechtigten (§ 303e Absatz 1 SGB V). Zudem soll die Stelle das Verfahren evaluieren und weiterentwickeln. Im Rahmen der Antragsprüfung hat das Forschungsdatenzentrum das Reidentifizierungsrisiko bei jeder Datenpreisgabe zu „bewerten und unter angemessener Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen zu minimieren" (§ 303d Absatz 1 Nr. 5). Die Speicherdauer ist maximal 30 Jahre (§ 303d Absatz 4). Die Forderung nach einer Verlängerung dieser Aufbewahrungsfristen steht im Raum.[5]

Die Liste der potenziell Nutzungsberechtigten ist lang (§ 303e Absatz 1): GKV-Spitzenverband, Bundes- und Landesverbände der Krankenkassen, Kassenärztliche Bundesvereinigung und Kassenärztliche Vereinigungen, Spitzenorganisationen der Leistungserbringer auf Bundesebene, Stellen zur Gesundheitsberichterstattung (Statistik, Bund und Länder), Einrichtungen unabhängiger wissenschaftlicher Forschung (incl. Hochschulen), gemeinsamer Bundesausschuss (gBA), Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG), Institut des Bewertungsausschusses (InBA), Patienten- und Behindertenbeauftragte (Bund, Länder), Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG), Institut für das Entgeltsystem im Krankenhaus (INEK GmbH), oberste Bundes- und Landesbehörden (also z. B. das BMG), Bundeskammern der Ärzte, Zahnärzte, Psychotherapeuten und Apotheker, Deutsche Krankenhausgesellschaft (DKG). Neu ist die Empfangsbefugnis von öffentlich geförderten außeruniversitäten Forschungseinrichtungen, also z. B. der Fraunhofer-Gesellschaft, der Helmholtz-Gesellschaft, der Leibniz-Gemeinschaft sowie der Max-Planck-Gesellschaft.[6]

Als Nutzungszwecke werden in § 303e Absatz 2 aufgeführt: Steuerungsaufgaben durch die Kollektivvertragspartner, Verbesserung der Versorgungsqualität, Planung von Leistungsressourcen (z. B. Krankenhausplanung), Unterstützung politischer Entscheidungen, Analyse und Entwicklung sektorenübergreifender Versorgungsformen und von Krankenkassen-Einzelverträgen, Gesundheitsberichterstattung sowie generell die Forschung.

Für diese Zwecke liefert das Forschungsdatenzentrum Auswertungen „anonymisiert und aggregiert" (§ 303e Absatz 3). Heikel ist, dass das Forschungsdatenzentrum auch pseudonymisierte Einzeldatensätze bereitstellen darf. Dafür muss ein Antragsteller darlegen, dass dies „für einen nach Absatz 2 zulässigen Nutzungszweck, insbesondere für die Durchführung eines Forschungsvorhabens, erforderlich ist". Der Nutzer muss „einer Geheimhaltungspflicht nach § 203 des Strafgesetzbuchs unterliegen" und technisch-organisatorisch gewährleisten, dass Datenminimierung praktiziert wird (§ 303e Absatz 4).

Die Nutzenden sollen auf die Einzeldatensätze nur unter Kontrolle des Forschungsdatenzentrums verarbeiten dürfen, was über einen „Gastarbeitsplatz in den Räumen des Forschungsdatenzentrums oder über einen gesicherten Fernzugriff" stattfinden soll. Die Nutzung der erlangten Daten ist nur zweckgebunden zulässig; die Nutzenden haben „darauf zu achten, keinen Bezug zu Personen, Leistungserbringern oder Leistungsträgern herzustellen" (§ 303e Absatz 5).

§ 303a Absatz 4 ermächtigt das BMG in Abstimmung mit dem Bundesforschungsministerium (BMBF) zum Erlass einer Rechts-

verordnung zwecks Konkretisierung der Verfahren (Datenumfang, Pseudonymisierungsverfahren, Bereitstellung von Einzeldatensätzen, Aufbewahrungsfrist, Evaluation, Weiterentwicklung). Gemäß § 303d Absatz 2 wird ein Arbeitskreis der Nutzungsberechtigten eingerichtet, der „an der Ausgestaltung, Weiterentwicklung und Evaluation des Datenzugangs" beratend mitwirkt.

3 Bewertung

Tatsächlich wird im Forschungsdatenzentrum eine zentrale Datensammlung von hochsensiblen Gesundheitsdaten von sämtlichen in Deutschland gesetzlich Versicherten auf- bzw. ausgebaut. Falsch ist, wie von Kritikern manchmal suggeriert wird, dass damit dem Missbrauch Tür und Tor geöffnet wird. Doch trotz der vorgesehenen Vorkehrungen bestehen rechtliche und voraussichtlich auch praktische Defizite. Anders als viele Kritiker halte ich die Nutzung der GKV-Gesundheitsdaten für Forschungszwecke für sinnvoll, wenn diese zur Weiterentwicklung unseres Gesundheitssystems und zum Fortschritt im Bereich der medizinischen Forschung genutzt werden. Ohne valide statistische Daten, die im medizinischen Bereich äußerst differenziert sein müssen, ist eine qualifizierte Gesundheitsberichterstattung nicht möglich.[7] Diese ist nötig als Grundlage für eine gerechte und effiziente staatliche Politik, für die Justierung des Abrechnungssystems sowie für das Erkennen von grundlegenden Entwicklungen und Zusammenhängen.[8]

Eingriffe in das Recht auf informationelle Selbstbestimmung sind aber nur zulässig, wenn diese im überwiegenden Allgemeininteresse erfolgen und hinreichende technisch-organisatorische und verfahrensrechtliche Vorkehrungen getroffen werden.[9]

Im deutschen Datenschutzrecht hatte bisher bei Forschungsnutzungen die Einwilligung absoluten Vorrang.[10] Dem gegenüber sieht Artikel 5 Absatz 1 lit. b DSGVO eine grundsätzliche und generelle Erlaubnis einer Zweitnutzung von personenbeziehbaren Daten für Forschungszwecke vor. Die DSGVO ist erheblich forschungsfreundlicher als das bisherige deutsche Recht, indem sie zwar Garantien für die Betroffenen fordert, nicht aber deren Zustimmung. Damit soll die Repräsentativität von wissenschaftlichen Auswertungen gesichert werden. Auch wenn für einen Ausgleich zwischen Forschungsfreiheit und Datenschutz gemäß der DSGVO eine generelle Widerspruchsmöglichkeit nicht zwingend ist, sind Vorkehrungen zum Betroffenenschutz nötig, etwa eine erhöhte Transparenzpflicht gepaart mit einem projektspezifischen Widerspruchsrecht.[11] Dass den Betroffenen im DVG überhaupt keine Rechte zugestanden werden, ist ein berechtigter Kritikpunkt an den Regelungen zur Datentransparenz.

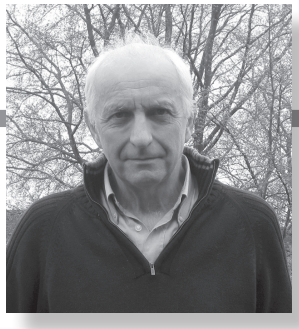
Für die meisten der nutzungsberechtigten Stellen genügen aggregierte, also vollständig anonymisierte Auswertungsergebnisse. Diese Stellen werden im Gesetz mit Forschenden in eine Reihe gestellt, die wichtige Fragestellungen oft nur mit personenbeziehbaren Einzeldatensätzen beantworten können. So öffnet der Gesetzestext die Tür für die Übermittlung von Einzeldatensätze an Stellen, die diese definitiv nicht erhalten sollten.

Das DVG erlaubt nicht nur die aggregierte Datennutzung, sondern auch die Auswertung von Einzeldatensätzen, wenn nachvollziehbar dargelegt wird, dass diese für einen zulässigen Nutzungszwecke erforderlich sind. Die Hürden für die Weiternutzung der Einzeldatensätze sind denkbar niedrig: 1. Die Empfänger müssen einer beruflichen Schweigepflicht unterliegen. 2. Die Datenminimierung muss technisch-organisatorisch abgesichert werden. 3. Es besteht eine gewisse Zweckbindung sowie 4. ein Reidentifizierungsverbot (§ 303e Absatz 4, 5). Eine saubere Abschottung, also eine räumliche, organisatorische und personelle Trennung zwischen der Erfüllung der operativen Aufgaben einer Stelle und der pseudonymen Verarbeitung von Transparenzdaten[12] ist nicht vorgesehen; ebenso fehlen sonstige wirksame Vorkehrungen gegen eine Reidentifizierung der pseudonymen Daten.[13]

Die Sicherheitsvorkehrung, dass eine Auswertung der für den jeweiligen Nutzenden freigeschalteten Einzeldatensätzen nur auf dem IT-System des Forschungszentrums zulässig sein soll, scheint wenig praxistauglich zu sein. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) soll die technische Sicherheit der technischen Analyseplattform des Forschungsdatenzentrums gewährleisten. Wenn Forschende Pseudonymdatensätze nicht mitnehmen können, um sie weiter auszuwerten, dürften sie viele wichtige Fragestellungen nicht oder nur schwer bearbeiten können.

Das Forschungsdatenzentrum hat das „spezifische Reidentifikationsrisiko in Bezug auf die durch Nutzungsberechtigte nach § 303e beantragten Daten zu bewerten" (§ 303d Absatz 1 Nr. 5). D. h. Risikobewertung, Fehler- bzw. Risikobehebung und Evaluation sollen in einer Hand liegen. Dies ist ein Unding. Hier bedarf es der Einschaltung einer unabhängigen Kontrollinstanz. Es ist nicht damit zu rechnen, dass der Verordnungsgeber eine solche künftig vorsehen wird (§ 303a Absatz 4 Nr. 4).

Die Sicherung der Vertraulichkeit über den Verweis auf die berufliche Schweigepflicht ist nicht ausreichend: § 203 StGB hat als



Thilo Weichert

Dr. **Thilo Weichert**, Netzwerk Datenschutzexpertise, 2004 bis 2015 *Landesbeauftragter für Datenschutz Schleswig-Holstein*, Vorstandmitglied der *Deutschen Vereinigung für Datenschutz e. V. (DVD)*.

Sanktionsinstrument derzeit in der Praxis keine bzw. nur symbolische Bedeutung; Ermittlungen sind selten; Sanktionierungen sind die absolute Ausnahme.[14]

Für die Datentransparenz sind keinerlei spezifischen Kontrollmechanismen vorgesehen. Dieses Defizit wird auch nicht durch eine verstärkte Datenschutzkontrolle kompensiert. Bei hochsensitiven, zentralisierten hoheitlichen Formen der Datenverarbeitung, die keinen sonstigen öffentlichen Kontrollmechanismen oder einer hinreichenden Transparenz unterliegen, hat das BVerfG gegenüber dem generellen Aufsichtsinstrumentarium verstärkte Maßnahmen gefordert, etwa kontinuierliche Regelkontrollen.[15]

Ungenügend sind auch die vorgesehenen Transparenzmaßnahmen. Das vorgesehene öffentliche Antragsregister (§ 303d Absatz 1 Nr. 6) mit Angaben zu Nutzungsberechtigten, Vorhaben und deren Ergebnissen[16] ist für eine wirksame Hinterfragung ungeeignet, solange nicht erkennbar ist, inwieweit welche Einzeldatensätze von den Nutzenden verarbeitet wurden.

Der Gesetzgeber hat sich nicht an ein Grundsatzproblem herangetraut, indem er es offen lässt, wann ein Forschungsprojekt in den Genuss eines privilegierten Datenzugangs kommen darf. Das BVerfG hat Forschung beschrieben als einen auf wissenschaftlicher Eigengesetzlichkeit (Methodik, Systematik, Beweisbedürftigkeit, Nachprüfbarkeit, Kritikoffenheit, Revisionsbereitschaft) beruhenden Prozess zum Auffinden von Erkenntnissen, ihrer Deutung und ihrer Weitergabe. Wissenschaftliche Forschung ist „alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist".[17] Es gibt in Deutschland aber keine Stelle und kein Verfahren, mit dem diese Anforderungen an privilegierte Forschung festgestellt und überprüft werden. Hierfür bedarf es aber klarer Kriterien, Regeln und Prozesse.[18] Für den Zugang zu den sensitiven GKV-Transparenzdaten verlangt das DVG nicht mehr, als dass die Forschung öffentlich gefördert wird. Dabei handelt es sich ausschließlich um einen finanziellen Aspekt, bei dem der Grundrechtsschutz keine Rolle spielt und ein öffentliches Interesse (der Institution, nicht des konkreten Projekts) allenfalls zu vermuten ist. Aus Sicht des Grundrechtsschutzes ist es nötig, dass Anforderungen an die Unabhängigkeit, die Transparenz, die Sicherungsvorkehrungen und das öffentliche Interesse des konkreten Projektes gestellt werden und diese im Rahmen eines administrativen Vorgangs geprüft, festgestellt und evtl. sanktioniert werden.

4 Ergebnis

Das Digitale-Versorgung-Gesetz ist mit seinen Regelungen zur Datentransparenz schlecht gemacht. Es gibt sich zwar nominell Mühe, Vorkehrungen zum Datenschutz zu treffen. Dabei fällt auf, dass vorrangig technische Maßnahmen vorgesehen sind. Das Instrument der Pseudonymisierung wird als Generalwaffe zur Verhinderung des individualisierten Datenmissbrauchs in Stellung gebracht. Für diesen grundsätzlich zu begrüßenden technischen Schutz wird aber kein administrativer Unterbau geschaffen. Pseudonymisierung generell wie im einzelnen Projektfall setzt Kompetenz, Dokumentation, Erprobung und Kontrolle voraus und gibt es nicht zum Nulltarif. Die Reidentifizierung pseudonymer Daten ist mit modernen Methoden der Auswertung oft ein Kinderspiel. Sollte das DVG und dessen Datentransparenz beim Bundesverfassungsgericht oder dem Europäischen Gerichtshof auf den Prüfstand gestellt werden, so dürfte dies schlecht für das Spahn´sche Projekt ausgehen, da die technisch-organisatorischen und prozeduralen Anforderungen ungenügend für den Grundrechtsschutz der GKV-Versicherten sind. Damit wird letztlich dem berechtigten Anliegen, eine bessere Datenbasis für die medizinische Forschung zu schaffen, ein Bärendienst erbracht.

Es ist erschreckend, mit welcher Unkenntnis die Politik mit den Bedürfnissen medizinischer Forschung und des Datenschutzes umgeht. Nicht praktikabel dürfte sich die Nutzung der Datentransparenz für die medizinischen Forschung erweisen, bei der es um ein Verschneiden von Klinikdaten mit GKV-Daten geht. Da das Digitale-Versorgungs-Gesetz nun mal in Kraft ist, muss dessen Umsetzung jetzt aufmerksam, fachkundig und kritisch begleitet werden. An Problembewusstsein hierfür scheint es bei vielen Stellen noch zu fehlen. Letztlich muss aber nicht nur das Bewusstsein der Beteiligten erhöht werden; nötig ist ein völlig neues gesetzliches Austarieren von Forschungsfreiheit und Datenschutz, gerade hier im medizinischen Bereich.

Anmerkungen

1 *G. v. 09.12.2019, BGBl. I S. 2562.*
2 *Weichert ZD 2020, 20.*
3 *BT-Drs. 19/13438, S. 71.*
4 *BT-Drs. 19/13438, S. 72.*
5 *Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF), Stellungnahme v. 09.10.2019, BT-Ausschuss f. Gesundheit, Ausschussdrucksache 19(14)105(12), S. 5.*
6 *BT-Drs. 19/13438, S. 74.*
7 *Weichert, Big Data im Gesundheitsbereich, 2018, https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf, S. 45 f., 163 f.*
8 *BVerfG 15.12.1983 – 1 BvR 209/83 u. a. (Volkszählung), Rn. 105, NJW 1984, 423.*
9 *BVerfG 15.12.1983 – 1 BvR 209/83 u. a., LS. 2, NJW 1984, 419.*
10 *Weichert/Bernhardt/Ruhmann, Die Forschungsklauseln im neuen Datenschutzrecht, 18.10.2018, https://www.netzwerk-datenschutz-expertise.de/sites/default/files/gut_2018_forschungklauseln_181018.pdf, S. 5.*
11 *Krawczak/Weichert, DANA 4/2017, 199.*
12 *BVerfG 15.12.1983 – 1 BvR 209/83 u. a., Rn. 109 ff., NJW 1984, 423.*
13 *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Stellungnahme vom 23.10.2019, S. 5.*
14 *Fischer, Strafgesetzbuch, 66. Aufl. 2019, § 203 Rn. 5.*
15 *BVerfG 24.03.2013 – 1 BvR 1215/07, Rn. 116 f. (Antiterrordateigesetz), NJW 2013, 1504.*
16 *Ebenso TMF (En. 5).*
17 *BVerfGE 35, 112 f. = NJW 1978, 1176; Werkmeister/Schwaab CR 2019, 85; Roßnagel, ZD 2019, 158f.; ähnlich Art. 2 lit. b Richtlinie 2005/71/EG des Rates über ein besonderes Zulassungsverfahren für Drittstaatsangehörige zum Zweck der wissenschaftlichen Forschung v. 12.10.2005, zur Erfordernis der Staatsferne Weichert, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, 231 f.; Britz in Dreier, GG Bd. I, 3. Aufl. 2013, Art. 5 III (Wissenschaft), Rn. 74 f.*
18 *Weichert ZD 2020, 23 f*

Jan Kuhlmann

Überblick über die Protestbewegung gegen die Telematikinfrastruktur

Der Verein *Patientenrechte und Datenschutz e. V.* hat *Forderungen für die einrichtungsübergreifende elektronische Gesundheitsakte* veröffentlicht.[1] Es müsse erreicht werden, dass bei der Gestaltung von Datensammlungen auf zentralen Servern folgende Rechte der Versicherten gewahrt bleiben:

- das Recht auf Vertraulichkeit (Arztgeheimnis),
- das Recht auf strikte Beachtung der Zweckbindung der Patientendaten,
- das Recht auf freie Arztwahl,
- das Recht, keine elektronische Gesundheitsakte zu haben,
- das Recht auf volle Verfügung über die eigene Akte.

Zu den Einzelmaßnahmen, die der Verein fordert, gehört das Recht der Versicherten, Daten einzelner Behandler komplett aus ihrer Behandlungshistorie zu löschen. Im Grunde wären dezentrale, von den Versicherten selbst organisierte Datensammlungen besser, um die Selbstbestimmung der Versicherten über ihre Gesundheit sicherzustellen.

Die Frage ist immer, ob und wie man solche Ziele und Utopien politisch wirksam machen kann. Erstaunlich ist immerhin, dass einiges aus den Forderungen seinen Weg in Gesetzentwürfe und öffentliche Auseinandersetzungen gefunden hat.

Die politischen Auseinandersetzungen um die Telematik-Infrastruktur sind derzeit überwiegend geprägt durch Initiativen von Psychotherapeutinnen und Psychotherapeuten sowie Ärztinnen und Ärzten gegen ihren Zwang zum Anschluss an die Telematik-Infrastruktur. Ende 2019 wurde eine Petition beim Bundestag eingereicht, in der gefordert wird: „Strafen gegen Ärzte und Psychotherapeuten, die sich nicht an die TI anschließen lassen, dürfen nicht verschärft, sondern müssen abgeschafft werden."[2]

Über 70.000 Unterschriften sind darunter gesammelt worden. Mehrere Ärztegruppen führen Musterklagen gegen den Honorarabzug von 2,5 % des Umsatzes, den Behandelnde zahlen müssen, die sich nicht an die Telematik anschließen. Über die Petition ist noch nicht entschieden worden.

Derzeit gibt es zwei verschiedene Bündnisse, die gegen die Telematik-Infrastruktur streiten, wie sie derzeit geplant ist:

- Das Bündnis *Stoppt die E-Card* existiert bereits seit 2007. Auch das FIfF ist dort Mitglied, wie viele andere Bürgerrechts-Organisationen. Seit einigen Jahren erschöpft sich die Tätigkeit dieses Bündnisses darin, einmal im Jahr eine Veranstaltung mit um die 50 Teilnehmerinnen und Teilnehmern durchzuführen, und gelegentlich eine Pressemitteilung des Vereins *Patientenrechte und Datenschutz* zu unterzeichnen. Seine Website[3] ist überwiegend veraltet.

- Das Deutsche Psychotherapeuten-Netzwerk[4] hat Ende 2019 die Initiative ergriffen, ein neues Bündnis mit ähnlichen Zielen zu gründen[5]. Dazu hat es 2020 zwei Treffen gegeben.

Personen, die *nur* als Versicherte von der Telematik-Infrastruktur betroffen sind, sind in beiden Bündnissen deutlich in der Minderheit. Gewerkschaftliche Initiativen zum Thema gibt es nicht. Obwohl die DGB-Gewerkschaften in den Selbstverwaltungsgremien der Krankenkassen bedeutend vertreten sind, sind eigenständige politische Ansätze zur Technisierung des Gesundheitswesens bei ihnen kaum vorhanden.

Eine überschaubare Anzahl von Aktiven zum Thema verfolgt derzeit drei Schwerpunktthemen:

- Entwicklung einer gemeinsamen Stellungnahme von Bürgerrechtsorganisationen zum neuen Gesetzentwurf der Bundesregierung, *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur*, um damit die Diskussion über die weitere Entwicklung dieser Infrastruktur zu beeinflussen,

- Vorbereitung einer Verfassungsbeschwerde gegen das Anfang 2020 verabschiedete *Patientendaten-Schutzgesetz*, insbesondere gegen die verpflichtende Weitergabe von Gesundheitsdaten zu Forschungszwecken ohne Einspruchsmöglichkeit der Betroffenen,

- Vorbereitung einer eigenen Kandidatur bei den Sozialwahlen 2023.

Es bleibt spannend.

Anmerkungen

1 *https://patientenrechte-datenschutz.de/informationen/forderungen-zur-einrichtungsuebergreifenden-e-gesundheitsakte/*
2 *https://epetitionen.bundestag.de/petitionen/_2019/_09/_02/Petition_98780.html*
3 *https://www.stoppt-die-e-card.de*
4 *https://kollegennetzwerk-psychotherapie.de/index.php?page=1586445332*
5 *http://gesundheitscloud.info*

Jan Kuhlmann

Jan Kuhlmann, geb. 1955, Jurist und Datenschutz-Berater. Seit 1992 aktiv zum Thema Datenverarbeitung im Gesundheitswesen. Mitarbeit an Veröffentlichungen, z. B. *Der Gesundheitschip – vom Arztgeheimnis zum gläsernen Patienten* (Campus-Verlag 1995), *Die neue elektronische Gesundheitskarte – The same procedure as every year?* (FIfF e. V. 2010), *Forderungen für die einrichtungsübergreifende elektronische Gesundheitsakte* (Patientenrechte und Datenschutz e. V. 2018)

NETZPOLITIK.ORG

Ingo Dachwitz

Datenschutz-Folgenabschätzungen: Vertrauen ist gut, Kontrolle ist besser

Neue Technologien wie Corona-Tracing-Apps rufen Misstrauen hervor. Ein bislang unterschätztes Instrument der Datenschutzgrundverordnung könnte mehr Transparenz und damit Vertrauen schaffen.

Seit Wochen diskutiert Deutschland über Corona-Apps[1]. Die Anwendungen sollen das Nachverfolgen von Infektionsketten erleichtern und dabei helfen, die Kontaktpersonen von Covid19-Erkrankten zu informieren. Doch die Verunsicherung ist groß: Wie weit lässt man den Staat mit den Programmen auf das eigene Smartphone? Wer garantiert für die Sicherheit der sensiblen Informationen über Gesundheitszustand und soziale Netzwerke? Was, wenn Regierungen der Versuchung nicht widerstehen können und doch mehr Informationen über BürgerInnen sammeln wollen als angekündigt?

„Wer in dieser Zeit eine Corona-App auf den Markt bringt, muss Transparenz schaffen", fordert deshalb Benjamin Bergemann vom Verein Digitale Gesellschaft. Der Politikwissenschaftler gehört zu einer Reihe von AktivistInnen, die in der Krise auf das Potenzial eines neuen und zugleich alten Datenschutzinstruments hinweisen. Es könnte helfen, die Vertrauensfrage zu beantworten: die Datenschutz-Folgenabschätzung (DSFA).

Was sperrig klingt, ist im Grunde einfach erklärt: Wer in der EU Datenverarbeitungen plant, die mit einem potenziell hohen Risiko für Grundrechte und Freiheiten einhergehen, ist nach der Datenschutzgrundverordnung (DSGVO) verpflichtet[2], vorab eine umfassende Selbstkontrolle durchführen. In Rahmen dieser Folgenabschätzung müssen Unternehmen, Vereine und staatliche Stellen systematisch auflisten, welche Verarbeitungsprozesse sie für die persönlichen Daten zu welchem Zweck planen. Außerdem müssen sie Risiken für die Betroffenen analysieren und Maßnahmen beschreiben, mit denen sie diese Risiken minimieren.

Transparenz ermöglicht Kontrolle, Kontrolle schafft Vertrauen

Die Folgenabschätzung ist Teil des sogenannten Risiko-basierten Ansatzes der DSGVO. Sie soll dem sperrigen Gesetz eine gewisse Flexibilität ermöglichen: DatenverarbeiterInnen müssen sich vorab selbst intensiv Gedanken machen und eigenständig Schutzmaßnahmen entwickeln. Wenn sie zu dem Schluss kommen, dass das Risiko trotzdem hoch bleibt, müssen sie die Aufsichtsbehörden konsultieren[3].

Eine Veröffentlichung der DSFA allerdings sieht die Datenschutzgrundverordnung nicht vor. Benjamin Bergemann hat deshalb beim Robert Koch-Institut eine Anfrage nach dem Informationsfreiheitsgesetz (IFG)[4] gestellt, um die Folgenabschätzung der Datenspende-App aus den Aktenordnern der Infektionsbehörde zu befreien. „Es gibt ein hohes öffentliches Interesse daran, nachzuvollziehen, dass die App datenschutzfreundlich entwickelt wurde. Die vom Robert Koch-Institut veröffentlichten Datenschutzinformationen erfüllen diesen Anspruch nicht", so Bergemann. Auch der Chaos Computer Club kritisierte die mangelhafte Transparenz[5] der Anwendung.

Einen anderen Weg ist das Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung gegangen. Da die Corona-Tracing-Apps in Deutschland selbst noch nicht fertiggestellt sind, haben die DatenschützerInnen des Vereins einfach selbst eine Folgenabschätzung erstellt[6] – ein Debattenbeitrag über die gesellschaftlichen Risiken dieser Technologien, der den MacherInnen der App gleichzeitig als konkrete Anregung dienen soll.

In dem gut hundert Seiten starken Dokument kamen die ExpertInnen schon sehr früh in der Debatte zu dem Schluss, dass es aus Sicht des Datenschutzes erhebliche Unterschiede mit sich bringt, ob ein dezentrales oder ein (teil-)zentralisiertes Modell[7] umgesetzt wird. Doch auch beim dezentralen Modell stellt die Folgenabschätzung erhebliche Risiken fest, für die der Verein jeweils konkrete Schutzmaßnahmen vorschlägt.

Licht in die Black Box bringen

Moderne Informations- und Kommunikationstechnologien sind für die wenigsten Menschen gänzlich durchschaubar. Eigentlich würde man erwarten, dass die allgegenwärtigen Datenschutzerklärungen hier einen Beitrag leisten würden. Ihre Veröffentlichung ist nach der DSGVO zwar verpflichtend, doch weil sie meist nicht zur Aufklärung, sondern zur rechtlichen Absicherung verfasst werden, erfüllen sie diesen Anspruch nur selten.

Gerade bei komplexen datenbasierten Systemen, die heute oft die Label Big Data oder Künstliche Intelligenz tragen, könnte die DSFA deshalb eine Möglichkeit sein, gesellschaftliche Auswirkungen überhaupt erst diskutierbar zu machen. „Viele solcher

Systeme operieren als ‚Black Boxes' – undurchsichtige Software-Werkzeuge, die sich aussagekräftiger Überprüfung und Verantwortlichkeit entziehen", schrieben Kate Crawford und Meridith Whitthaker 2018 in einem Bericht über automatisierte Entscheidungssysteme[8]. Die Forscherinnen des US-amerikanischen Think Tanks AI NOW brachten deshalb *Algorithmic Impact Assesments* ins Spiel. Folgenabschätzungen, die dem Privacy Impact Assessment der DSGVO nicht unähnlich sind.

Tatsächlich steht die DSFA in der Tradition der parlamentarischen Technik-Folgenabschätzung, bei der es nicht nur um einzelne Datenverarbeitungen, sondern um die Diskussion gesellschaftlicher Konsequenzen geht. Vor dem Hintergrund der Debatte um die kommerzielle Nutzung von Atomenergie habe sich dieses Instrument seit den 70er Jahren etabliert, um „die Chancen und Risiken der Technik für die Gesellschaft sowie deren Akzeptanz […] unter einem ganzheitlichen und damit interdisziplinären Winkel" zu erforschen, erklärt das Forschungsprojekt *Forum Privatheit* in einem White Paper[9].

Bereits seit Ende 70er Jahre sei dieses Element auch schon in einigen deutschen Datenschutzgesetzen angelegt gewesen, wurde jedoch nie wirklich entfaltet. Erst mit der Datenschutzgrundverordnung wird der alten Idee neues Leben eingehaucht.

Als führe man den TÜV in der eigenen Garage durch

Ein Gespräch mit Stefan Brink zeigt: Überall angekommen ist das noch nicht. Doch die Zahl der DatenverarbeiterInnen, die selbstständig eine DSFA durchführen, nehme kontinuierlich zu, berichtet der Landesdatenschutzbeauftragte von Baden-Württemberg. Wann das notwendig ist, definiert die DSGVO nicht genau, Orietierung geben Handreichungen der Aufsichtsbehörden[10]. Im Vergleich zu den Vorabkontrollen, die das alte Bundesdatenschutzgesetz vorgesehen hatte, habe sich die Zahl der Folgenabschätzungen jedenfalls mehr als verdoppelt, so Brink.

Bislang behalten DatenverarbeiterInnen die Dokumente jedoch lieber für sich. Eine Praxis, die auch Lea Pfau vom Transparenzportal *Frag den Staat* kritisiert. Es sei nur schwer vorstellbar, dass Verantwortliche in der Selbstprüfung jemals zu dem Ergebnis kämen, dass sie die Aufsichtsbehörde konsultieren müssen, weil sie das Risiko nicht in den Griff bekommen: „Das wäre ungefähr so, als würde man den TÜV für sein Auto in der eigenen Garage selbst durchführen."

Eine Veröffentlichung der Abschätzung erfülle jedoch nicht nur eine Kontrollfunktion. Die Transparenzmaßnahme könne zudem die Qualität des Datenschutzes verbessern, weil es einen Feedback-Kanal gebe. Das gelte besonders im Fall der Corona-Apps: „Das öffentliche Interesse geht hier einher mit einem erheblichen Maß an vorhandener Expertise", so Pfau.

„Wer nach außen demonstrieren will, dass man Datenschutz kapiert hat, hat mit Veröffentlichung der Folgenabschätzung ein ideales Werbemittel, um die eigene Seriosität zu demonstrieren", findet auch Stefan Brink, der in Baden-Württemberg nicht nur Beauftragter für Datenschutz, sondern auch für Informationsfreiheit ist. „Anstatt sich wegzuducken, kann man sich demonstrativ offen zeigen. Nach dem Motto: Prüft uns, macht Verbesserungsvorschläge." Brink bestätigt derweil, dass es so gut wie nie vorkomme, dass Unternehmen seine Behörde in Folge der internen Folgenabschätzung konsultieren würden.

Security by Obscurity ist eine schlechte Ausrede

Zumindest die Datenschutz-Folgenabschätzung von Behörden seien in der Regel IFG-pflichtig, bestätigt Stefan Brink. Dass das in der Praxis durchaus anders aussehen kann, zeigt ein Fall aus der Redaktion von netzpolitik.org: Als Kollegin Anna Biselli beim Bundesamt für Migration und Flüchtlinge per IFG die Datenschutz-Folgenabschätzungen von IT-Assistenzsystemen[11] anfragte, mit der etwa die Herkunft von AsylbewerberInnen plausibilisiert werden soll, wurde sie zunächst fast ein ganzes Jahr hingehalten. Am Ende wurde die Anfrage abgelehnt, da die Bekanntgabe des Inhalts der Folgenabschätzung die öffentliche Sicherheit gefährden könne. Dritte könnten mit ihr „mögliche Sicherheitslücken der Datenverarbeitung" aufspüren und ausnutzen.

Dieses Argument bekomme er öfter zu hören, sagt Datenschutz-Aktivist Benjamin Bergemann. Doch davon solle man sich nicht blenden lassen: „Wer auf *Security by Obscurity* setzt, hat ohnehin ein Problem." IT-Sicherheitsarchitekturen sollten nicht davon abhängen, dass sie undurchschaubar seien. Allerdings könne man über die Detailtiefe der Informationen einer veröffentlichten DSFA diskutieren, da hier nicht der einzelne Verarbeitungsvorgang, sondern der Grundrechtsschutz insgesamt im Vordergrund stehe.

Diese Sichtweise unterstützt auch die Rechtsanwältin Nina Diercks. Sie berät regelmäßig Unternehmen in Datenschutzfragen und auch bei der Erstellung von DSFA. Da die Folgen-

Ingo Dachwitz

Ingo Dachwitz ist Medien- und Kommunikationswissenschaftler, Redakteur bei *netzpolitik.org* und Mitglied beim Verein *Digitale Gesellschaft*. Er schreibt und spricht über Datenpolitik, Überwachungskapitalismus und den digitalen Strukturwandel der Öffentlichkeit. Ingo gibt Workshops für junge und ältere Menschen in digitaler Selbstverteidigung und lehrt manchmal an Universitäten zur politischen Ökonomie digitaler Medien. Gelegentlich moderiert er auch Veranstaltungen und Diskussionen, etwa auf der *re:publica* oder beim *Netzpolitischen Abend* in Berlin. Ingo ist Mitglied der sozialethischen Kammer der EKD und berät kirchliche Organisationen bei der digitalen Transformation. Kontakt: Ingo ist per Mail an *ingo | ett | netzpolitik.org* (PGP-Key[14]) erreichbar und als *@roofjoke* auf Twitter unterwegs.

abschätzung ohnehin in vielen Fällen vorgenommen werden müsse, sei der Weg zur Veröffentlichung nicht mehr weit. Notfalls könnten Verantwortliche die Folgenabschätzung um sicherheitsrelevante Aspekte bereinigen und eine leicht abgespeckte Variante veröffentlichen, so Diercks.

Österreich macht es vor

Dass das Robert Koch-Institut die Folgenabschätzung der Datenspende-App nicht proaktiv veröffentliche, sei wenig vertrauensbildend, findet Diercks. Auch Bergemann sieht die Behörden bei Corona-Apps in einer Bringschuld. „Das sind Hochrisiko-Technologien, die flächendeckend eingesetzt werden sollen. Da muss der Staat gegenüber den Bürgern nachweisen, dass sie grundrechtskonform funktionieren."

Folgenabschätzungen seien kein Allheilmittel, doch sie würden Technologien und ihre Folgen überhaupt erst diskutierbar machen – „eine Voraussetzung dafür, dass wir sie gesellschaftlich kontrollieren können." Inzwischen fordert auch der Europäische Datenschutzausschuss[12], also das Gremium aller nationalen Datenschutzaufsichtsbehörden der EU, die Veröffentlichung der Folgenabschätzungen für Tracing-Apps.

Wie das konkret aussehen kann, demonstriert in Österreich das Rote Kreuz. Schon früh hatte die Organisation zusammen mit der Beratungsfirma Accenture in der Alpenrepublik die „Stopp Corona"-App an den Start gebracht. Mitte April wurde die gut 100 Seiten starke Folgenabschätzung veröffentlicht. Mehrere NGOs konnten zudem den (inzwischen ebenfalls veröffentlichten) Source Code einsehen und haben die Anwendung auf dieser Basis geprüft[13].

Ihr Fazit: Es gibt Verbesserungsvorschläge, aber alles in allem ist die Anwendung sicher und datenschutzfreundlich. Wer dem Urteil der ExpertInnen nicht traut, kann sich nun immerhin selbst ein Bild machen. Denn Vertrauen ist gut – Kontrolle ist besser.

Quelle: https://netzpolitik.org/2020/datenschutz-folgenabschaetzung-dsgvo-vertrauen-ist-gut-kontrolle-ist-besser/

Anmerkungen

1 *https://netzpolitik.org/2020/faq-corona-apps-die-wichtigsten-fragen-und-antworten-zur-digitalen-kontaktverfolgung-contact-tracing-covid19-pepppt-dp3t/*
2 *https://dsgvo-gesetz.de/art-35-dsgvo/*
3 *https://dsgvo-gesetz.de/art-36-dsgvo/*
4 *https://fragdenstaat.de/anfrage/datenschutz-folgenabschatzung-zur-corona-datenspende-app/*
5 *https://netzpolitik.org/2020/die-datenspende-app-braucht-mehr-transparenz/*
6 *https://www.fiff.de/presse/dsfa-corona/*
7 *https://netzpolitik.org/2020/welche-technologie-bietet-den-besseren-datenschutz/*
8 *https://ainowinstitute.org/aiareport2018.pdf*
9 *https://www.forum-privatheit.de/download/datenschutz-folgenabschaetzung-3-auflage-2017/*
10 *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236*
11 *https://fragdenstaat.de/anfrage/datenschutz-folgeabschatzungen/*
12 *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf*
13 *https://epicenter.works/sites/default/files/analyse_stopp_corona_app_v1.0.pdf*
14 *https://pgp.mit.edu/pks/lookup?op=get&search=0x05550760A5E4E814*

Tomas Rudl

Die Krise als Hebel für Überwachung und Kontrolle

Weltweit bauen demokratische Staaten Grundrechte ab, um gegen das Coronavirus vorzugehen. Manchen Regierungen scheint das aber nur ein vordergründiges Anliegen zu sein. Leichtfertig abgesegnet könnten temporäre Maßnahmen zur Dauereinrichtung werden – und zum Schuss ins eigene Knie.

Ein ausgeschaltetes Parlament, langjährige Haftstrafen für das Verbreiten von „Falschnachrichten" oder für Verstöße gegen das Ausgehverbot: So weit wie das von Viktor Orbán regierte Ungarn ist bislang noch kein EU-Land gegangen, um die Coronakrise einzudämmen. Sollte das Parlament dem Gesetzentwurf nächste Woche mit der notwendigen Zweidrittelmehrheit zustimmen – wovon Beobachter des Landes ausgehen[1] –, dann hätte Ungarn bis auf Weiteres sein demokratisches und schon länger humpelndes Experiment beendet.

In aller Welt versuchen derzeit die Regierungen[2], schnell die richtige Antwort auf die Pandemie zu finden. Manche, darunter Orbáns rechte Fidesz-Partei, scheinen eher die Gunst der Stunde zu nutzen, um ihre Macht abzusichern und ihre Kritiker zum Verstummen zu bringen, als mit demokratischen Mitteln die aktuelle Gesundheitskrise in den Griff zu bekommen.

Nicht unähnlich die Situation in Israel: Dort setzt die Regierung des Premiers Benjamin Netanyahu höchst invasive Techniken ein, die das Land sonst im Anti-Terror-Kampf nutzt[3]. Dem Inlandsgeheimdienst ist nun unter anderem erlaubt[4], sämtliche Handys des Landes zu tracken, ohne die Daten zuvor zu anonymisieren[5]. Das soll dazu dienen, die Einhaltung der Quarantäne zu überprüfen und gegebenenfalls Infektionsketten nachzuverfolgen.

1. Staaten könnten bleibende Fakten schaffen

Solche Meldungen lassen vielerorts die Alarmglocken schrillen. „Ich befürchte, in den nächsten Wochen und Monaten wird ungefähr jede vorstellbare digitale Überwachungsmaßnahme ins Spiel gebracht werden", sagt der Überwachungsexperte Wolfie

Christl. „Es besteht die Gefahr, dass Firmen und Staaten dabei bleibende Fakten schaffen. Viel mehr noch als nach 9/11."

Bislang blieb Deutschland von überbordenden und drakonischen Maßnahmen weitgehend verschont, selbst wenn der eine oder andere Testballon aufgestiegen[6] ist. Dennoch kommt es auch hierzulande zu Grundrechtseinschränkungen[7], etwa zu Ausgangssperren. Das mag gerechtfertigt erscheinen, um eine Gesundheitskatastrophe zu verhindern.

Allerdings mahnte jüngst die Rechtswissenschaftlerin Andrea Edenharter[8], die Balance zu wahren: „Ebenso wie eine bloße *laissez faire*-Strategie fehl am Platze wäre, darf in die Freiheitsrechte der Bürger trotz der Krise nicht in verfassungswidriger Weise eingegriffen und auf diese Weise eine faktische Entmündigung der Bevölkerung vorgenommen werden."

2. Aktionismus wirkt oft

Zuweilen nehmen solche Bestrebungen beinahe amüsante Ausmaße an. In Polen beispielsweise müssen in Heim-Quarantäne gesteckte Bürger via Selfie nachweisen, sich tatsächlich zu Hause aufzuhalten. Antworten sie nicht innerhalb von 20 Minuten oder verweigern die Installation der dazu notwendigen App, dann hört der Spaß schnell auf[9]: Sie müssen mit einem Polizeibesuch und Geldstrafen rechnen.

Wenig zu lachen hatten auch Menschen, die aufgrund überstürzter Grenzschließungen nicht nach Hause konnten und Schleichwege nehmen mussten. Wie in einem Film aus Zeiten des Kalten Krieges soll es an der deutsch-polnischen Grenze ausgesehen haben, berichtet die Historikerin Anne Applebaum[10]. Straßensperren und bewaffnete Streifen sollten ein Gefühl der Sicherheit vermitteln.

Dass es dabei zu einer laut dem Deutschen Roten Kreuz „humanitär bedenklichen Situation" gekommen ist, die eher Aktionismus als eine wirksame Maßnahme gegen die Corona-Ausbreitung war und die Sperren inzwischen gelockert[11] werden mussten, scheint keine große Rolle gespielt zu haben. In Krisenzeiten eignet sich Symbolpolitik[12] hervorragend dazu, das Image eines „Machers" zu stärken – wie es dem rechtskonservativen polnischen Präsidenten Andrzej Duda bislang gelungen ist, der sich im Mai seiner Wiederwahl stellen will und in Umfragen meilenweit vorne liegt.

Selbst US-Präsident Donald Trump, der noch vor wenigen Wochen die Coronakrise als einen von den Medien inszenierten „Hoax" bezeichnete, seinen wissenschaftlichen Beratern das Leben zur Hölle[13] macht und neuerdings (mit einiger Sicherheit fälschlicherweise) davon ausgeht, die Krise bis Ostern[14] bewältigt zu haben, kann sich über Höhenflüge in Meinungsumfragen[15] freuen. 60 Prozent der Befragten bescheinigen ihm derzeit, gute Arbeit in der Krisensituation geleistet zu haben. Nichtsdestotrotz unternahm sein Justizminister Bill Barr kürzlich einen ersten Versuch, die Situation für massive Grundrechtseinschränkungen[16] zu nutzen, scheiterte vorerst aber an parlamentarischem Widerstand.

„Wir müssen wachsam sein", sagte der Soziologe Richard Sennett dem Tagesspiegel[17]. Der Brite macht sich Sorgen darum, dass die Notfallmaßnahmen, wie sie nun überall ergriffen werden, dauerhaft installiert bleiben. „Mehr Überwachung, mehr Kontrolle könnte die bisherigen Regelungen ersetzen, legitimiert durch die Krise, aber über ihre zeitlichen Grenzen hinaus", warnt Sennett.

3. Südkorea will Überwachungspraxis überdenken

Dabei ist gar nicht sichergestellt, dass rigorose Überwachung tatsächlich mehr hilft als schadet. In Südkorea etwa, das von CDU-Gesundheitsminister Jens Spahn am Montag lobend für sein Handy-Tracking erwähnt wurde, kam es zu einer Reihe an Datenschutzskandalen[18]. Leichtfertig veröffentlichte Details aus dem Privatleben von möglicherweise mit dem Coronavirus Infizierten führten zu Online-Hetzjagden, Verschwörungstheorien und Erpressungsversuchen.

Der Himmel über Seoul – Foto: Nina Evensen

Und letztlich zu der Ankündigung der südkoreanischen Gesundheitsbehörden, ihre bisherige Praxis überarbeiten zu wollen[19]. Sie fürchten, die Vorfälle könnten Menschen davon abhalten, sich testen zu lassen – was die bis dahin geschafften Erfolge umgehend zunichte machen könnte.

Ohnehin scheinen ganz andere Faktoren ausschlaggebend für den Erfolg[20] zu sein als eine lückenlose Überwachungsmaschine-

Tomas Rudl

Tomas Rudl ist in Wien aufgewachsen, hat dort für diverse Provider gearbeitet und daneben Politikwissenschaft studiert. Seine journalistische Ausbildung erhielt er im Heise-Verlag, wo er für die *Mac & i*, *c't* und *Heise Online* schrieb. Er ist unter +49-30-92105-9861 oder *tomas@netzpolitik.org* (PGP-Key[22]) erreichbar und twittert mal mehr, mal weniger unter *@tomas_np*.

rie: ein gut ausgebautes Gesundheitssystem etwa samt ausreichenden Testkapazitäten; handlungsfähige Behörden, die rasch eventuell Infizierte ausfindig machen und sie gegebenfalls isolieren; und ein politisches System, das seinen Bürgern vertraut und umgekehrt[21].

Quelle: https://netzpolitik.org/2020/die-krise-als-hebel-fuer-ueberwachung-und-kontrolle/

Anmerkungen

1 *https://www.derstandard.at/story/2000116068044/ungarn-vor-der-diktatur*
2 *https://privacyinternational.org/examples/tracking-global-response-covid-19*
3 *https://www.washingtonpost.com/world/middle_east/israel-turns-to-anti-terrorism-tools-in-battle-against-coronavirus/2020/03/15/3670bd94-66b9-11ea-b199-3a9799c54512_story.html*
4 *https://www.timesofisrael.com/high-court-green-lights-phone-surveillance-after-knesset-oversight-panels-formed/*
5 *https://netzpolitik.org/2020/zeig-mir-deinen-standort-und-ich-sage-dir-ob-du-vielleicht-krank-bist/*
6 *https://netzpolitik.org/2020/jens-spahn-laesst-testballon-steigen/*
7 *https://www.zeit.de/gesellschaft/zeitgeschehen/2020-03/coronavirus-ueberblick-eu-grenzkontrolle-ausgangssperre-bussgelder*
8 *https://verfassungsblog.de/freiheitsrechte-ade/*
9 *https://www.france24.com/en/20200320-selfie-app-to-keep-track-of-quarantined-poles*
10 *https://www.theatlantic.com/ideas/archive/2020/03/when-disease-comes-leaders-grab-more-power/608560/*
11 *https://www.rbb24.de/studiofrankfurt/panorama/coronavirus/corona-verkehr-autobahn-polen-grenze-lkw.html*
12 *https://www.zeit.de/politik/ausland/2020-03/coronavirus-osteuropa-ukraine-ungarn-polen-demokratie-pandemie-folgen/komplettansicht*
13 *https://www.politico.com/news/2020/03/05/trump-coronavirus-scientists-on-edge-122121*
14 *Der Beitrag wurde am 26. März 2020 veröffentlicht.*
15 *https://news.gallup.com/poll/298313/president-trump-job-approval-rating.aspx*
16 *https://www.politico.com/news/2020/03/21/doj-coronavirus-emergency-powers-140023*
17 *https://www.tagesspiegel.de/kultur/richard-sennett-zur-corona-krise-wir-muessen-wachsam-sein/25657932-all.html*
18 *https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives*
19 *https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html*
20 *https://www.washingtonpost.com/world/europe/germany-coronavirus-death-rate/2020/03/24/76ce18e4-6d05-11ea-a156-0048b62cdb51_story.html*
21 *https://netzpolitik.org/2020/durch-solidaritaet-koennen-wir-einen-ausnahmezustand-verhindern/*
22 *https://pgp.mit.edu/pks/lookup?op=get&search=0x745121858AE13AED*

Julia Barthel

Es fehlt die direkte Kommunikation

Digitaler Unterricht in Zeiten von Corona

Lernplattformen gibt es schon lange, die Coronakrise verlangt der Infrastruktur an den Schulen aber mehr ab. LehrerInnen und SchülerInnen müssen miteinander kommunizieren – am besten funktioniert das, wenn man sich gegenseitig sieht. Wir haben nachgefragt, wo es bereits Videokonferenzsysteme gibt.

Mitte März wurde klar, dass die Schulen schließen müssen, um die Ausbreitung des Coronavirus einzudämmen. Viele Schulen haben versucht, auf digitalen Unterricht umzustellen. Dazu greifen sie auf bereits bestehende Lernplattformen zurück, die, teils mit durchwachsenem Erfolg[1], einen guten Teil der Aufgaben bewältigen können.

Dennoch haben selbst etablierte Werkzeuge ihre Defizite. Vor allem fehlen ihnen Tools zur direkten Kommunikation, etwa über Videotelefonie, und auch der Datenschutz hat nicht immer Priorität. Diese Situation kritisieren auch SchülerInnen selbst[2].

Viele SchülerInnen fühlen sich alleine gelassen[3]: „Zwischen dem alleinigen Aufgaben erledigen und einer Unterrichtsstunde befinden sich Welten.", erklärt Moritz Masch vom Brandenburger Schülerrat[4]. Die „gesamte Verantwortung für den Lernerfolg" werde gerade den SchülerInnen aufgebürdet, schreibt die LandesschülerInnenvertretung NRW: „Hinzu kommt ein überfülltes Postfach von SchülerInnen und LehrerInnen, mit 20 Nachrichten, die alle bearbeitet und beantwortet werden müssen."

Eine Kommunikationsplattform für individuelle Fragen[5] wünscht sich die Landesschülervertretung Thüringen, eigene E-Mail-Adressen für alle SchülerInnen fordert der Landesschülerrat Brandenburg.

Solide Grundlage

Die meisten Bundesländer betreiben für ihre Schulen die Lernplattform „Moodle"[6] oder ein ähnliches System. Dort können NutzerInnen Material wie Aufgaben oder Dokumente austauschen und Arbeitsgruppen bilden. Baden-Württemberg stellt jeder Schule eine eigene *Moodle*-Instanz[7] zur Verfügung, Rheinland-Pfalz[8] ist nach eigenen Angaben selbst an der Entwicklung der Open-Source-Software beteiligt, in Bayern ist sie in das landeseigene System *mebis*[9] integriert.

Für Videokonferenzen mussten einige Länder kurzfristig die kommerzielle Video-Erweiterung *Webex* von Cisco kaufen, so in Berlin[10], Schleswig-Holstein[11] oder Rheinland-Pfalz. Aller-

dings sollen die meisten dieser Systeme laut den zuständigen Ministerien nur für eine Übergangszeit die hohen Zugriffszahlen abfangen. Langfristig soll die offene Software *BigBlueButton*[12] oder *Jitsi Meet*[13] auf landeseigenen Servern bereitgestellt werden.

Bis über die Plattform *it's learning*[14] des Landes Bremen Videokonferenzen möglich sind, arbeiten die Schulen dort mit der kommerziellen Software *Zoom*, teilte die Senatorin für Schule mit. Diese Entscheidung sei in Abstimmung mit dem Finanzsenator sowie mit einem externen Datenschutzbeauftragten[15] getroffen worden.

Auf unsere Nachfrage gab die Bremer Datenschutzbeauftrage an, dass sie nicht in die Entscheidung einbezogen wurde, den Einsatz von Zoom aber für „nicht unbedenklich" halte: Der Quellcode sei weder einsehbar noch überprüfbar, zudem würden mindestens die Metadaten auf US-amerikanischen Servern verarbeitet.

Eigene Videokonferenzsysteme sind Realität

Datenschutzfreundlicher sind selbstgehostete Videokonferenzsysteme, wie es sie mit BigBlueButton in Sachsen[16] und Sachsen-Anhalt schon gibt. Getestet wird noch in Baden-Württemberg, im Saarland[17] oder in Thüringen[18]. Dahinter stehe die Idee einer eigenverantwortlichen Schule, erklärt das Schulministerium aus Sachsen-Anhalt und verweist auf die Leitlinien zur IT-Ausstattung von Schulen[19].

Außerdem habe BigBlueButton auch gegenüber kommerziellen Alternativen einen größeren Funktionsumfang, man könne Präsentationen hochladen, anzeigen und zum Herunterladen freigeben, Abfragen durchführen oder gemeinsam auf ein Whiteboard schreiben. Die Thüringer Landesschülervertretung begrüßt außerdem die Datenschutzfreundlichkeit eigener Plattformen[20].

LehrerInnen sollen sich kümmern

Trotzdem darf die Verantwortung nicht auf die Schulen abgeschoben werden, sondern die Bundesländer brauchen eine klare Strategie für die schulische Infrastruktur. Gar kein Videokonferenzsystem bietet bisher Mecklenburg-Vorpommern, hier „dürfen" LehrerInnen selbst entscheiden. Aktuell laufe ein Vergabeverfahren für ein landesweites Lern-Management-System, heißt es aus dem Ministerium.

Auch in Hessen und Bayern gibt es bisher keine Videokonferenzsysteme des Landes. Bayern empfiehlt in einem Schreiben an alle Schulen[21] mögliche ergänzende Werkzeuge wie „cloud-gestützte Office-Produkte, ggf. mit Videokonferenzsystem (zu denken wäre hier zum Beispiel an Microsoft Office 365) oder datenschutzfreundliche Messenger-Dienste". Hessen sieht zwar, dass Werkzeuge für Einzel- und Gruppenchats, für Videokonferenzen und kollaboratives Arbeiten hilfreich sein können, bleibt aber bei einem allgemeinen Verweis auf die Softwarelösungen Jitsi und BigBlueButton.

Foto: Thomas Gerlach

Digitalisierung geht nicht von alleine

Mal eben schnell digitalisieren ist meist wenig datenschutzfreundlich. Das zeigte bereits die Plattform *Logineo* des nordrhein-westfälischen Schulministeriums[22], die seit 2018 an ausgewählten Schulen im Testbetrieb läuft. Seither steht sie in der Kritik[23], weil LehrerInnen die Sicherheit vertraulicher SchülerInnendaten auf ihren privaten Endgeräten garantieren sollten – nach Einschätzung verschiedener Lehrerverbände ein untragbarer Zustand. Sie forderten stattdessen Dienstgeräte.

Auch die LandesschülerInnenvertretung NRW spricht sich dagegen aus, dass SchülerInnen ihre eigenen Geräte[24] nutzen sollen, weil nicht jedeR einen eigenen, leistungsfähigen Laptop oder Computer besitze und einzelne SchülerInnen unter Umständen ausgeschlossen würden.

Ehrenamt und Eigenmotivation

Dass Technik nicht alles ist, zeigen auch sechs „Didaktische Hinweise" für LehrerInnen[25] des Schulministeriums NRW. Darin heißt es auch: „So viel Empathie und Beziehungsarbeit wie möglich, so viele Tools und Apps wie nötig."

Trotzdem müssen diese nötigen Tools datenschutzfreundlich bereitgestellt werden – und auch bei den SchülerInnen ankommen. Denn gerade hängt es von den einzelnen Schulen oder vom Engagement einzelner LehrerInnen ab, welche Software eingesetzt wird. Besonders gut läuft es dort, wo Ehrenamtliche Lücken mit eigener Infrastruktur stopfen oder LehrerInnen hohe Eigeninitiative zeigen.

Achtung vor „kostenfrei"

Solche Initiativen brauchen mehr Unterstützung, weil Digitalisierung kostet. Auch wenn für freie Software wie Moodle, BigBlueButton oder Jitsi Meet keine Lizenzgebühr fällig wird, müssen Hardware oder Administrationsdienstleistungen bezahlt werden. Bisher kümmern sich häufig Lehrkräfte um die IT-Systeme ihrer Schulen. Für Logineo NRW etwa werden sie dafür eine Stunde wöchentlich vom Unterricht freigestellt[26].

Die Landesschülervertretung NRW warnt andererseits vor kommerziellen Plattformen, die ihrer Einschätzung nach die Chance nutzen wollen, Marktanteile zu gewinnen und daher kostenfreie Lockangebote[27] zur Verfügung stellen: „Was auf den ersten Blick wie ein großzügiges Angebot wirkt, ist tatsächlich ein weiterer Schritt zur Privatisierung und Gewinnorientierung der Bildungsinfrastruktur."

Was wird tatsächlich gebraucht und hilft in der Krise weiter? Auch wir versuchen, positive Beispiele aufzuzeigen[28] und haben dafür bereits mit Stefan Kaufmann aus Ulm[29] und Steffen Haschler aus Mannheim[30] gesprochen. Sind Sie selbst Eltern oder LehrerInnen? Wo läuft es besonders gut? Berichten Sie uns von Ihren Erfahrungen.

Quelle: https://netzpolitik.org/2020/es-fehlt-die-direkte-kommunikation/

Anmerkungen

1 *https://www.br.de/nachrichten/netzwelt/warum-die-lernplattform-mebis-noch-immer-eine-baustelle-ist*
2 *https://www.lsvrlp.de/de/article/4069.bildung-trotz-pandemie-aber-wie.html*
3 *https://lsvnrw.de/positionen/presse/bildungspolitische-forderungen-in-der-coronakrise/#more-5910*
4 *https://www.lsr-brandenburg.de/pressemitteilungen/lernen-von-zuhause-aus/*
5 *https://xn--lsv-thringen-ilb.org/corona-lernen*
6 *https://de.wikipedia.org/wiki/Moodle*
7 *https://www.schule-bw.de/service-und-tools/webtools/moodle*
8 *https://lernenonline.bildung-rp.de/*
9 *https://www.mebis.bayern.de/*
10 *https://www.lernraum-berlin.de/*
11 *https://schullogin.de/*
12 *https://de.wikipedia.org/wiki/BigBlueButton*
13 *https://de.wikipedia.org/wiki/Jitsi*
14 *https://hb.itslearning.com/*
15 *https://www.bildung.bremen.de/start-1459*
16 *https://www.opal-schule.de/*
17 *https://online-schule.saarland/*
18 *https://www.schulportal-thueringen.de/thueringer_schulcloud*
19 *https://edulabs.de/blog/Open-Source-Software-und-Hardware-in-der-Schule*
20 *https://xn--lsv-thringen-ilb.org/corona-lernen*
21 *https://www.km.bayern.de/download/22787_Coronavirus_Einsatz-digitaler-Medien-12.03.2020.pdf*
22 *https://www.logineo.schulministerium.nrw.de/LOGINEO/index.html*
23 *https://www.nw.de/nachrichten/zwischen_weser_und_rhein/22624483_Datenschuetzer-warnen-vor-der-digitalen-Schulplattform-Logineo-NRW.html*
24 *https://lsvnrw.de/positionen/presse/bildungspolitische-forderungen-in-der-coronakrise/#more-5910*
25 *https://www.schulministerium.nrw.de/docs/Recht/Schulgesundheitsrecht/Infektionsschutz/300-Coronavirus/Coronavirus_Impulse_Distanzlernen/index.html*
26 *https://www.schulministerium.nrw.de/docs/Schulpolitik/LOGINEO-NRW/index.html*
27 *https://lsvnrw.de/positionen/presse/bildungspolitische-forderungen-in-der-coronakrise/#more-5910*
28 *https://netzpolitik.org/2020/helft-mit-schulen-brauchen-offene-infrastrukturen/*
29 *https://netzpolitik.org/2020/ulm-baut-offene-bildungsinfrastruktur-fuer-schulen/*
30 *https://netzpolitik.org/2020/in-mannheim-kommt-das-digitale-und-offene-klassenzimmer/*

Julia Barthel

Freie Software in der digitalen Lehre: Ganz nach Bedarf

Während die meisten Unis komplett auf externe Anbieter wie Zoom oder Microsoft Teams setzen oder einzelne Lizenzen zukaufen, läuft digitale Lehre an der Uni Osnabrück vollständig mit freier Software auf eigenen Systemen. Wie das geht, erklärt Andreas Knaden im Interview.

In unserer Reihe Offene Bildungsinfrastrukturen wollen wir Einblicke in erfolgreiche Bildungsprojekte geben, die mit Open-Source-Technologien offene und datenschutzfreundliche Lösungen entwickeln. Für dieses Interview haben wir mit Andreas Knaden gesprochen, der an der Universität Osnabrück das Rechenzentrum und das Zentrum für digitale Lehre, Campus-Management und Hochschuldidaktik (virtUOS) leitet. Ersteres kümmert sich um die technische Infrastruktur, letzteres um die didaktische Aufbereitung der Inhalte.

netzpolitik.org: *Welche Strategie verfolgt die Uni Osnabrück, wenn es um digitale Lehre geht?*

Andreas Knaden: Über die Jahre haben wir gelernt, dass wir mit Open-Source-Produkten sehr viel näher an das herankommen, was von den AnwenderInnen benötigt wird. Denn digitale Lehre verändert sich stark. Da setzen wir auf Open-Source-Produkte, weil wir sie für uns anpassen können – viel mehr als solche von einem anderen Hersteller. Wir versuchen außerdem, diese Projekte nachhaltig zu integrieren. Wir haben gesehen, dass es Lehrenden wie Studierenden schwer fällt, wenn man einen Flickenteppich aus Werkzeugen liefert. Viel schneller und effizienter geht es, wenn alles miteinander verbunden und ineinander eingebettet ist. Ein Beispiel: Die Videokonferenzsysteme, die wir verwenden, sind integriert in die Lernplattform. Das heißt: Wenn ich in einer Lehrveranstaltung bin und in das entsprechende Videokonferenzsystem hineingehe, sind da sofort die Rechte für meine Studierenden und für mich als Lehrender implementiert. Ich muss keine neue Gruppe bilden oder irgendwas verschicken, sondern das ist alles direkt nutzbar.

netzpolitik.org: *Sie sind selbst mit Ihrem Team an der Entwicklung von Software beteiligt – zum Beispiel bei der Lehrplattform Stud.IP. Wie kam es denn dazu? Ist das normal für eine Uni, dass man mitentwickelt?*

Andreas Knaden: Das ist letztlich eine Frage der Infrastruktur, des Personals und der Interessenlage. Bei uns war von Anfang an der Gedanke, dass wir Forschung und Unterstützung der Lehre miteinander verbinden wollen. Und wenn Sie forschen, dann ist es spannend, den Forschungsgegenstand auch verändern zu können. Wenn man diesen Gedanken zu Ende verfolgt, muss man eigentlich was mit Open Source machen. Da können wir tatsächlich Dinge modifizieren: Wir nehmen Anforderungen entgegen, probieren in einer ersten Näherung etwas aus und verändern dann die Systeme entsprechend den Bedarfen. Der andere Punkt ist: Wir haben gesehen, dass im Open-Source-Bereich viele andere Universitäten mit im Boot sind. Das vermindert unseren Aufwand. Wir basteln nicht irgendeine private Lösung, sondern wir haben immer Teams aus mehreren Hochschulen.

netzpolitik.org: *Welche Anwendungen stellt die Uni Osnabrück ihren Studierenden denn zur Verfügung?*

Andreas Knaden: Das ist ein ganzer Mix aus Werkzeugen, für das Studieren im Netz, aber auch für die Präsenzlehre. Ich fange mal bei den Vorlesungsaufzeichnungen an. Der Bereich ist bei uns ganz groß und wir haben mit OpenCast selbst Software mitentwickelt, die weltweit im Einsatz ist. Damit können Lehrende im Hörsaal, oder auch am heimischen PC, ihre Lehrveranstaltung aufzeichnen und sie an beliebig viele Studierende streamen. In diesem Semester besonders wichtig ist das Werkzeug Meetings, das in unsere Lernplattform Stud.IP eingebaut ist. Dahinter steckt BigBlueButton als Open-Source-Lösung für Videokonferenzen. Und natürlich haben wir die üblichen Dinge: einen Datenbereich, einen Chat, Etherpad-Plugins – eine breite Palette von Werkzeugen, alle in einer Plattform.

netzpolitik.org: *Wie haben Sie entschieden, welche Werkzeuge Sie einsetzen?*

Andreas Knaden: Es gibt Experimentalphasen, wo wir in kleinen Gruppen ein Werkzeug ausprobieren. Wir schauen uns an, ob das angenommen wird und wie die Studierenden und die Lehrenden damit umgehen können. Eigentlich sind wir dauernd auf der Suche nach Dingen, die wir in der Lehre brauchen können. Und daraus ergibt sich dann im Laufe der Zeit ein Mix an Werkzeugen, mit dem wir arbeiten. Was letztlich in der Lehrveranstaltung eingesetzt wird, bestimmen die Hochschullehrenden. Er greift in das Füllhorn, das wir anbieten.

netzpolitik.org: *Die meisten Unis haben Lizenzen zugekauft für Zoom oder Microsoft Teams. Das hat die Uni Osnabrück nicht gemacht. Kennen Sie noch weitere Unis, die rein auf freie Software und eigene Systeme setzen?*

Andreas Knaden: Ehrlich gesagt nicht. Viele haben allerdings nicht aus freiem Willen, sondern aus Not auf die kommerziellen Systeme zurückgegriffen, habe ich in Gesprächen mit anderen Hochschulen erfahren. Die waren einfach nicht in der Lage, schnell genug etwas Eigenes auf die Beine zu stellen. Das könnte wieder korrigiert werden angesichts der großen Kritik, der sich Zoom derzeit ausgesetzt sieht. Das könnte aber auch deswegen korrigiert werden, weil ich der festen Überzeugung bin, dass wir auf lange Sicht mit den Open-Source-Produkten sogar irgendwann mal ökonomisch günstiger fahren. Und dann ist fraglich, warum man sich an einen externen Anbieter wenden soll. Es ist ja auch durchaus angenehm zu wissen, dass alles, was an Daten über's Netz geht, bei einer Uni verarbeitet wird und nicht irgendwo im freien Raum.

netzpolitik.org: *Ist das zu viel verlangt von einer Uni, diese Ressourcen selbst bereitzustellen? Warum sind Sie da so eine Ausnahme?*

Andreas Knaden

Andreas Knaden: Das hängt damit zusammen, dass die Universität Osnabrück schon viele Jahre Erfahrung im Open-Source-Bereich hat. Wir haben uns in diesem Bereich einen qualifizierten Ruf aufgebaut und konnten so viele Projekte einwerben. Ich schätze mal, dass andere Hochschulen gar nicht so viel qualifiziertes Personal unmittelbar zur Verfügung haben. Deshalb weichen einige dann auf Standard-Produkte aus. Wir haben Glück und wir haben gut vorgearbeitet. Und wir haben ein sehr leistungsfähiges, neues Rechenzentrum.

netzpolitik.org: *Mit ihrem alten Rechenzentrum wäre das nicht gegangen?*

Andreas Knaden: Ich denke nicht. Wenn wir die alte Hardware beispielsweise hätten einsetzen müssen für OpenCast, BigBlueButton oder Stud.IP, hätte das mit Sicherheit zu Schwierigkeiten geführt. Etwa beschränkte Teilnehmendenzahlen bei der Nutzung der Videokonferenz, Geschwindigkeitseinbußen bei Stud.IP oder Kapazitätsgrenzen bei der Videoaufzeichnung. Stud.IP bei Volllast wird hier von 3.000 Studierenden gleichzeitig genutzt, vorher waren es vielleicht 1.400. Jetzt reagieren die Systeme mit zwei bis maximal drei Sekunden Reaktionszeit in der Volllastphase. BigBlueButton haben wir letzte Woche mit den Studierenden getestet. Wir hatten zwischen 1.700 und 1.800 Nutzende gleichzeitig im System und wir hatten noch Luft nach oben. Das wäre mit den alten Systemen nicht möglich gewesen.

netzpolitik.org: *Wie lief denn die erste Vorlesungswoche hier in Osnabrück?*

Andreas Knaden: Tatsächlich sehr entspannt und problemlos. Was die zentralen Server angeht, haben wir nirgends auch nur

annähernd eine Lastgrenze erreicht, sondern wir sind so zwischen zwanzig und dreißig Prozent Auslastung, wenn es wirklich mal hochkommt. In den Hochzeiten hatten wir eine Netzlast nach draußen, die unter 1,8 Gigabit lag. Wir haben 3 Gigabit zur Verfügung für den Download und derzeit 10 Gigabit für den Upload. Und von dieser 10 Gigabit-Grenze waren wir quasi 8 Gigabit pro Sekunde entfernt.

Das Hauptproblem bestand darin, dass viele Nutzende auf die Netzverbindungen bei ihnen zu Hause angewiesen sind. Und die arbeiten mit schlechten Leitungen an der Grenze dessen, was man im Moment machen kann. Das macht mich traurig und nachdenklich. Einige hat es auch bei der eigenen Hard- und Software ein bisschen kalt erwischt. Wer sich nicht so sehr für Technik interessiert, hat vielleicht nun mit der vorhandenen PC-Ausstattung Probleme. Was uns auch viel Mühe gemacht hat, sind dezentrale Firewalls, VPN-Systeme. Da mit den Nutzenden drüber zu sprechen und das zu korrigieren, ist nicht so einfach.

netzpolitik.org: *Wie kommen die Studierenden und Lehrenden insgesamt mit dem digitalen Lehrangebot zurecht?*

Andreas Knaden: Wir hatten hier Beratungsstunden, viele Schulungen und konnten viele Lehrende und Studierende auch erreichen. In der Info-Veranstaltung letzte Woche hatten insgesamt 1.600 Studierende, mit denen wir uns intensiv unterhalten haben. In ganz vielen Fällen sind die Rückmeldungen positiv. Man ist glücklich, dass es so gut funktioniert. Dann gibt es natürlich auch welche, die mit unlösbaren Problemen kommen, aber den meisten können wir helfen. Und ich glaube, das ist ganz wichtig, dass man in dieser Situation die Menschen auffängt, die mit ganz akuten Problemen kommen – das sind ja manchmal nur Kleinigkeiten, die verhindern, dass es läuft. Klar, es gibt auch Fälle, in denen wir nicht helfen können. Aber auch da gibt es dann Verständnis, dass es bei bestimmten Rahmenbedingungen nicht funktioniert.

Es gibt natürlich auch einige Lehrende, die sich vorher nicht so intensiv mit digitaler Lehre auseinandergesetzt haben und die – wenn auch nicht unbedingt mit Begeisterung – aber mit hohem Engagement dabei sind, sich die Technologien zu eigen zu machen. Ich habe sehr häufig in den letzten Tagen gehört: „Och, das ist ja alles gar nicht so schlimm." Die Studierenden machen das auch toll, weil sie ihre Lehrenden darin bestärken. Da gibt es viele Standing Ovations für Lehrende, die sich besondere Mühe geben.

netzpolitik.org: *Würden Sie sich wünschen, dass noch mehr Unis auf eigene Hardware und freie Software setzen?*

Andreas Knaden: Auf jeden Fall. Weil die dann alle auch potentielle KooperationspartnerInnen für Softwareentwicklung, Leistungsaustausch etc sind. Eigene Hardware ist noch ein anderes Thema. Ich bekomme von vielen Hochschulen Anfragen, ob wir unterstützen können mit unseren Kapazitäten – und das freut mich natürlich. Es könnte sein, dass sich in dem Bereich ein neues Geschäftsfeld auftut durch Hosting und Kooperation. Das wäre klasse und ist auch Teil eines Antrags, den wir in den vergangenen Wochen beim Ministerium platziert haben. Dann spezialisieren sich einige Unis auf bestimmte Hosting-Fragestellungen, Osnabrück beispielsweise für Teile der digitalen Lehre, und andere können konsumieren, ohne sich vertieft in die Dinge einarbeiten zu müssen.

netzpolitik.org: *Was war das für ein Antrag, den sie gestellt haben?*

Andreas Knaden: Wir sind von der Landeshochschulkonferenz aufgefordert worden, nochmal zu spezifizieren, was die Corona-Krise für uns als Hochschulen bedeutet – insbesondere finanziell. Welche Folgen dieser intensive Einsatz der digitalen Lehre für uns in den einzelnen Hochschulen hat und wie das perspektivisch zu sehen ist. Daraufhin haben wir uns mit mehreren Hochschulen zusammengesetzt und einen Fünfjahresplan geschrieben, mit dem wir durch entsprechende Förderung den Hochschulen Freiraum verschaffen wollen. Damit digitale Lehre jetzt einerseits keine Eintagsfliege ist und andererseits optimal gestaltet werden kann. Denn viele laufen jetzt mit ihren Standard-Ressourcen am Limit. Und wenn digitale Lehre tatsächlich jetzt an Ausbreitung gewinnt, werden sich Dinge massiv verändern. Nach Corona wird vieles in der Lehre nicht mehr so sein wie es vorher war. Es wird nicht rein digital, aber der digitale Anteil wird deutlich höher sein. Wenn das funktionieren soll, dann wird man in den digitalen Bereich investieren müssen.

Offenlegung: Die Autorin ist selbst eingeschriebene Studentin an der Universität Osnabrück.
Korrektur: Wir haben einige Aussagen von Andreas Knaden geändert, bei denen wir ihn missverständlich zitiert hatten.

Quelle: https://netzpolitik.org/2020/ganz-nach-bedarf/

Anmerkungen

1 *mailto:julia.barthel@netzpolitik.org*
2 *https://keys.openpgp.org/vks/v1/by-fingerprint/44835593CC79D15FCEF953A1C65F9EA5B121A4A0*

Julia Barthel

Julia Barthel ist von Mitte April bis Mitte Juli 2020 Praktikantin in der Redaktion von *netzpolitik.org*. Sie hat Germanistik und Soziologie studiert und fast einen Masterabschluss. Bei *Jugend hackt* hat sie 2017 endlich Menschen gefunden, um über Technik zu sprechen – und dann wurden es immer mehr. Außerdem recherchiert und redet sie gerne im Radio oder auf Bühnen; am liebsten über Gesellschaft, IT, Gleichberechtigung, Zugang zu Wissen und wie man alles besser machen kann. Sie ist per Mail[1] erreichbar, am liebsten verschlüsselt[2].

Matthias Monroy

INPOL-Datei: Deutlich mehr Gesichtserkennung bei Bundespolizei und Kriminalämtern

Die Abfragen von biometrischen Lichtbildern in der INPOL-Datei nehmen drastisch zu, bei der Bundespolizei haben sie sich im Vergleich zum Vorjahr mehr als verdreifacht. Immer öfter ist die Gesichtserkennung dabei erfolgreich, doppelt so viele Personen wie noch 2018 wurden identifiziert.

Polizeibehörden in Deutschland nutzen die Gesichtserkennung nicht in Echtzeit, sondern nur rückwirkend[1]. Mit der Technik sollen unbekannte Personen ermittelt werden, deren Fotos etwa in der Nähe von Tatorten durch Videoüberwachung im öffentlichen Raum aufgenommen wurden. Auch nach dem G20-Gipfel 2017 in Hamburg hatte die dortige Polizei mutmaßliche StraftäterInnen auf diese Weise ermitteln wollen, der Erfolg war allerdings mäßig[2].

Die biometrischen Gesichtsbilder, mit denen die Fotos Unbekannter verglichen werden, liegen in der Polizeidatenbank INPOL-Z. Sie wird beim Bundeskriminalamt (BKA) zwar zentral geführt, aber zusammen mit den Landeskriminalämtern betrieben. Auch die Bundespolizei kann darauf zugreifen. Die Zahl der in INPOL mit Personendaten abgelegten Lichtbilder ist mit rund 5,8 Millionen Portraitfotos zu 3,65 Millionen Personen abermals deutlich angestiegen. Gegenüber 2018 beträgt der Zuwachs etwa fünf Prozent (310.000 Bilder).

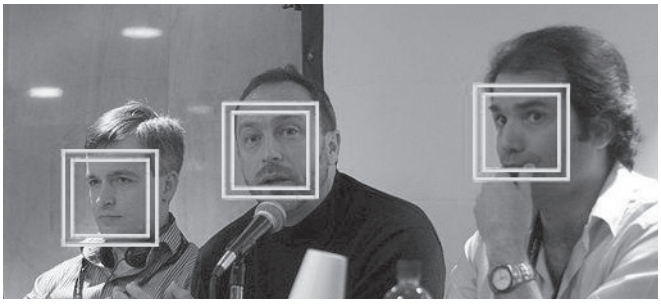
Unerklärliche Zunahme

Die Angaben stammen aus der Antwort[3] des Staatssekretärs im Bundesinnenministeriums, Hans-Georg Engelke, auf eine Kleine Anfrage. Einen Grund für die starke Zunahme nennt das Ministerium nicht. Die INPOL-Datei enthält vorwiegend Gesichtsbilder aus erkennungsdienstlichen Behandlungen, die aber innerhalb von bestimmten Fristen wieder entfernt werden müssen. Eine detaillierte Auswertung der „hinzugekommenen und gelöschten Lichtbilder" ist laut Engelke aber wegen der Corona-Lage „zurzeit nicht möglich".

Auch die Abfragen der 5,8 Millionen Lichtbilder über das beim BKA geführte Gesichtserkennungssystem (GES) nehmen stark zu. Dieser Trend zeigt sich jedes Jahr[4], für 2019 ist aber besonders die Zunahme bei der Bundespolizei auffällig. Deren Bild-Suchläufe waren mit rund 5.200 noch nie so hoch wie jetzt, im Vergleich zu 2018 haben sie sich sogar mehr als verdreifacht. Insgesamt hatten die deutschen Polizeien damals rund 54.000 Abfragen im GES gestartet.

Signifikant zugenommen hat außerdem die Zahl der Personen, die mithilfe der Gesichtserkennung identifiziert wurden. 2019 wurden über 2.100 auf diese Weise namhaft gemacht, doppelt so viele wie im Vorjahr. Hier erfolgte der Anstieg vor allem bei den Kriminalämtern.

Eine Erklärung für den Anstieg ist nicht bekannt, er mag an der stetig verbesserten Auflösung von Kameras liegen, möglicherweise ist aber auch die Software erneuert worden. Der Umstieg auf ein komplett neues Erkennungssystem, wie ihn das BKA vor einigen Jahren ins Auge fasste[5] und eine Studie dazu



Gesichtserkennung mit OpenCV
Foto: Beatrice Murch, derivative work: Sylenius CC BY 2.0

beauftragte, ist jedenfalls laut der nun vorliegenden Antwort nicht erfolgt.

BKA-Staatsschutz führt eigene Datei

Neben INPOL führt das BKA eine eigene, vergleichsweise kleine Datei ST-Libi-Z mit rund 3.500 Lichtbildern[6] zu fast 3.000 Personen aus dem Bereich der politisch motivierten Kriminalität mit Schwerpunkt „Religiöse Ideologie". Das *ST* steht für „Staatsschutz", das *Z* wie bei INPOL für „zentral". Zugriff darauf hat nur das BKA selbst, das „unbekannte polizeilich relevante Personen" identifizieren will.

In der *Libi*-Datei suchen die BKA-ErmittlerInnen händisch, also bei Ermittlungen für jeden Einzelfall. In 15 „dringenden" Fällen sind dort gespeicherte Personen aber mit dem Lichtbildbestand in INPOL-Z abgeglichen worden. *Libi* ermöglicht laut dem Bundesinnenministerium automatisierte Bildvergleiche. Damit könnte sie als Referenzdatei dienen, wenn die Bundespolizei einmal mit der automatisierten Gesichtserkennung im öffentlich Raum beginnt.

Quelle: https://netzpolitik.org/2020/deutlich-mehr-gesichtserkennung-bei-bundespolizei-und-kriminalaemtern/

Anmerkungen

1 *https://www.mdb-alexander-ulrich.de/fileadmin/lcmsulrich/user/upload/SF220.pdf*
2 *https://netzpolitik.org/2019/gesichtserkennung-hamburger-innenbehoerde-pfeift-auf-datenschutzbeauftragten/*
3 *https://www.andrej-hunko.de/start/download/dokumente/1475-speicherungen-in-polizeilichen-eu-datenbanken-2019*
4 *http://dipbt.bundestag.de/dip21/btd/19/012/1901261.pdf*
5 *https://netzpolitik.org/2018/gesichtserkennung-bka-will-auf-verbessertes-system-umstellen/*
6 *https://dipbt.bundestag.de/doc/btd/19/167/1916723.pdf*

Matthias Monroy

Wozu nutzt Interpol Gesichtserkennung?

Die internationale Polizeiorganisation entwickelt ein System, mit dem unbekannte Personen mithilfe von Lichtbildern identifiziert werden sollen. In einer Datei speichert Interpol Fotos und Videos, die von Internetanbietern und anderen Firmen stammen. Für die Gesichtserkennung hat Interpol auch Dienste von Clearview ausprobiert.

Die US-amerikanische Firma *Clearview AI* hat rund drei Milliarden Bilder von Menschen aus dem Internet eingesammelt und daraus eine Datenbank zur Gesichtserkennung erzeugt. Das hatte die New York Times vor sechs Wochen berichtet[1]. Die Bilder stammen größtenteils aus Profilfotos Sozialer Medien, vermutlich werden auch die dazugehörigen Nutzerdaten bei Clearview gespeichert. Clearview bietet Firmen und Behörden an, mit einer Abfrage der Datenbank Personen zu identifizieren. Die Gesichtsbilder können Berichten zufolge auch mit einer Foto-App abgefragt werden, die Anwendung ist der New York Times zufolge[2] unter „Reichen" verbreitet.

Das US-Magazin Buzzfeed ist an eine Kundenliste von Clearview gelangt[3]. Darauf stehen über 2.200 Firmen, Regierungen und Polizeibehörden, darunter auch Interpol. Die weltweit tätige Polizeiorganisation hat demnach mehr als 320 Suchanfragen durchgeführt.

„Monitoring-Plattformen, Industrie und kommerzielle OSINT"

Das Interpol-Generalsekretariat in Lyon hat den JournalistInnen bestätigt, dass „eine kleine Anzahl von Beamten" die Anwendung genutzt hat. Es gebe jedoch keine Geschäftsbeziehung mit Clearview, vielmehr habe es sich um einen kostenlosen 30-Tage-Probeaccount gehandelt.

Das ist plausibel, denn die Organisation entwickelt derzeit ein eigenes System zur Gesichtserkennung. Im April vergangenen Jahres startete Interpol das zweijährige Projekt DTECH, das Fotos und Videos aus Sozialen Medien verarbeitet. Interpol erhält die Dateien auf offiziellem Weg, schreibt das deutsche Bundesinnenministerium[4]. Demnach basiert DTECH auf Gesichtsbildern, die über „nationale Behörden, regionale Monitoring-Plattformen, Industrie und kommerzielle OSINT" bereitgestellt werden. Sie werden anschließend bei Interpol gespeichert.

Wie Clearview wird auch DTECH zur Identifizierung von Personen genutzt. Laut der Bundesregierung sollen damit unbekannten Personen „nominelle Daten" (also Personendaten, Ausweisnummern, etc.) zugeordnet werden. Allerdings ist nicht bekannt, mit welchen Referenzdateien bei Interpol die über DTECH erlangten Gesichter abgeglichen werden. Möglich wäre dies im Projekt *Facial, Imaging, Recognition, Searching and Tracking*[5] (FIRST), mit dem unbekannte Terrorismusverdächtige identifiziert werden sollen.

Neue Datei mit Fahndungsfotos

Einen ersten Anlauf startete FIRST in Gefängnissen im Niger. Interpol hat von dortigen Anti-Terrorismus-Behörden Gesichtsbilder erhalten und diese zunächst in eigenen Dateien gesucht. Anschließend wurden die Fotos unbekannter Personen als sogenannte *Blue Notices* zur Identifizierung und Aufenthaltsermittlung an die 192 Interpol-Mitgliedstaaten verteilt. Sofern die dortigen Behörden über ein Gesichtserkennungssystem verfügen, können die Fotos dort mit eigenen Beständen verglichen werden. Beim Bundeskriminalamt (BKA) ist dies die INPOL-Datei, dort sind derzeit rund 5 Millionen Gesichtsbilder durchsuchbar gespeichert.

Auch Interpol baut derzeit eine als *Criminal Information System* (ICIS) bezeichnete Datenbank mit Gesichtern auf. Dabei handelt es sich um Bilder, die im Rahmen von Fahndungsersuchen aus den Mitgliedstaaten ohnehin bei der Polizeiorganisation verfügbar sind. Sie werden auf ihre Eignung zur Gesichtserkennung überprüft und anschließend in einer eigenen „Gesichtserkennungsdatenbank" gespeichert. Im vergangenen Jahr waren dort rund 54.000 Personendatensätze mit durchsuchbarem Lichtbild[6] gespeichert.

Die neue Datei kann nach Angaben von Interpol[7] von den Behörden aller Interpol-Mitgliedstaaten abgefragt werden. Die dabei genutzte Software zur Gesichtserkennung *MorphoFace Investigate* stammt von der Firma Safran Identity and Security. Auch das BKA will die „Gesichtserkennungsdatenbank" nutzen, seit 2016[8] scheiterte dies aber aus Gründen des Datenschutzes. Fraglich ist das Verfahren[9], nachdem andere Polizeibehörden über „Treffer", also gefundene Gesichter, informiert wer-

Matthias Monroy

Matthias Monroy[7] Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift *Bürgerrechte & Polizei/CILIP*[8]. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Alle Texte unter *digit.so36.net*, auf englisch *digit.site36.net*, auf Twitter *@matthimon*. Viel zu selten auf der Straße (dafür im Internet) gegen Faschismus, Rassismus, Sexismus, Antisemitismus. Kein Anhänger von Verschwörungstheorien jeglicher Couleur. Benutzt das Binnen-I trotz Gepolter nervtötender Maskulisten.

den. Zuerst muss im BKA überprüft werden, ob es sich nicht um einen *false positive* handelt – also ein Gesicht irrtümlich „erkannt“ wurde.

Clearview will Bilder von Polizeien

Interpol betreibt mit den *Red Notices* außerdem eine Datenbank mit gesuchten und zur Verhaftung ausgeschriebenen StraftäterInnen. Jeder Mitgliedstaat kann diese Fahndungen an beliebige andere Interpol-Mitglieder verteilen. Denkbar ist, dass Interpol das Internet nach Informationen zu dort gespeicherten Personen durchsucht. Falls die Betroffenen beispielsweise über Accounts in Sozialen Medien verfügen, könnten diese Informationen bei der Aufenthaltsermittlung helfen. Eine derartige Nutzung bietet auch Clearview seinen NutzerInnen an.

Laut OneZero[10] bittet Clearview auch Polizeibehörden um Gesichtsbilder, das US-Magazin hat einen entsprechenden Mailwechsel über eine Informationsfreiheitsanfrage erhalten. Schon jetzt nutzen Clearview und seine Konkurrenten demnach Fahndungsfotos von abgegrasten Internetseiten, auf denen Bilder aus der erkennungsdienstlichen Behandlung durch US-Polizeien abrufbar sind. Eine ähnliche Datei[11] findet sich auch auf der Interpol-Webseite. Clearview könnte sich auf diese Weise als Hilfspolizistin andienen, indem etwa alle drei Milliarden Gesichtsbilder mit polizeilichen Fahndungen abgeglichen und etwaige Treffer an die Polizei verkauft würden.

Aus Datenschutzgründen dürften die Polizeien aber den eigenen Abgleich bevorzugen. Laut dem Hamburger Datenschutzbeauftragten Johannes Caspar wäre beispielsweise die Nutzung von Diensten wie Clearview nicht grundsätzlich problematisch. Rechtswidrig wäre aber, wenn die polizeilich abgefragten Gesichtsbilder bei einem privaten Anbieter liegen.

Arbeitsgruppe zur Gesichtserkennung

Für die verschiedenen Verfahren zur Gesichtserkennung hat Interpol eine *Facial Recognition Working Group* eingerichtet, an der auch das BKA teilnimmt. Zu den Sitzungen werden Polizeien aus Australien, Frankreich, Israel, Großbritannien und den USA eingeladen. Die Behörden stellen dabei neue Techniken und Anwendungsgebiete für Gesichtserkennung vor.

Die Themen der Gruppe hat das Bundesinnenministerium in der Antwort auf eine schriftliche Frage[12] benannt. Demnach erörtern die TeilnehmerInnen Möglichkeiten zur „Umsetzung der Gesichtserkennung auf nationaler Ebene“, die „Internationale Zusammenarbeit im Bereich der Gesichtserkennung und des Datenaustausches“ sowie „Entwicklungsschritte im Bereich der Gesichtserkennung“. Dort erlangte Informationen können „auch in die Weiterentwicklung nationaler Systeme einfließen“. Gut vorstellbar, dass auf einer dieser Sitzungen auch die Nutzung von Clearview behandelt wurde.

Quelle: https://netzpolitik.org/2020/wozu-nutzt-interpol-gesichtserkennung/

Anmerkungen

1 *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html*
2 *https://www.nytimes.com/2020/03/05/technology/clearview-investors.html*
3 *https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement*
4 *https://dip21.bundestag.de/dip21/btd/19/086/1908683.pdf*
5 *https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects*
6 *http://dipbt.bundestag.de/dip21/btd/19/059/1905954.pdf*
7 *https://www.interpol.int/How-we-work/Forensics/Facial-Recognition*
8 *http://dipbt.bundestag.de/doc/btd/18/106/1810604.pdf*
9 *http://dipbt.bundestag.de/doc/btd/19/019/1901908.pdf*
10 *https://onezero.medium.com/clearview-ai-we-are-working-to-acquire-all-u-s-mugshots-from-past-15-years-645d92319f33*
11 *https://www.interpol.int/How-we-work/Notices/View-Red-Notices*
12 *http://dipbt.bundestag.de/doc/btd/19/019/1901908.pdf*

Marie Bröckling

Neue Überwachungs-Werkzeuge für die saarländische Polizei

Mit Änderungen am Polizeigesetz will die schwarz-rote Landesregierung den Weg frei machen für neue Tools zur digitalen Beobachtung. Geplant sind unter anderem die anlasslose Videoüberwachung und die elektronische Fußfessel. Nicht nur der Paragraf zur geplanten Spähsoftware ist noch reichlich holprig.

Ein neues Polizeigesetz für das Saarland[1] könnte bereits in den nächsten Monaten im Landtag Saarbrücken verabschiedet werden. Der Polizei stünde dann neues technisches Equipment zur Verfügung, beispielsweise die elektronische Fußfessel, Bodycams und Spähsoftware.

Heute gaben eingeladene ExpertInnen ihre Verbesserungsvorschläge zu den geplanten Änderungen ab. Auch ich bin als Sachverständige im Innenausschuss und habe vorab eine schriftliche Stellungnahme eingereicht[2]. Hier die wichtigsten Punkte zusammengefasst.

Es gibt keine rechtliche Verpflichtung, polizeiliche Befugnisse auszubauen

In dem Gesetzentwurf aus dem CDU-geführten saarländischen Innenministerium heißt es, dass sich gesetzgeberischer Handlungsbedarf unter anderem aus dem Urteil des Bundesverfassungsgerichts zum BKA-Gesetz[3] ergebe. Diese Argumentation ist nicht neu: Immer wieder haben PolitikerInnen den Ausbau der polizeilichen Befugnisse in den letzten drei Jahren mit rechtlicher Notwendigkeit begründet[4].

Doch es gibt keine gesetzgeberische Verpflichtung, das rechtlich gerade noch Zulässige umzusetzen. Die VerfassungsrichterInnen in Karlsruhe zogen bei ihrem Urteil 2016 lediglich die Grenzen des polizeilichen Handelns, sie sprechen keine Empfehlungen aus. So formulierten sie etwa Auflagen für den Einsatz von Staatstrojanern.

Völlige Verwirrung bei Trojanersoftware

Im Urteil des Bundesverfassungsgerichts[5] zum BKA-Gesetz heißt es:

> *Das Gesetz lässt jedenfalls keinen Zweifel, dass eine Quellen-Telekommunikationsüberwachung nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt ist.*

Dennoch soll die saarländische Polizei Trojanersoftware einkaufen, um damit Handys oder Computer zu infiltrieren und verschlüsselte Messenger-Nachrichten auszulesen und sie soll – so will es die Landesregierung – „auch die bereits abgeschlossene und gespeicherte" Kommunikation überwachen und aufzeichnen dürfen, „soweit diese im überwachten System gespeichert sind".

Es ist fast so, als hätte die saarländische Landesregierung jahrelange Debatten um Quellen-TKÜ und Online-Durchsuchung verschlafen. Zumindest scheint sie sich der Tragweite dieses technischen Eingriffs nicht bewusst. Auf Nachfragen der Abgeordneten zur technischen Beschaffenheit kann ein Vertreter des Innenministeriums heute nicht antworten.

„Forderungen aus der Praxis"

Zudem will der Gesetzentwurf „Forderungen aus der Praxis" umsetzen[6]. Es sei eine „gute und konstruktive Zusammenarbeit bei der Erarbeitung" des neuen Polizeigesetzes gewesen, schreibt auch der saarländische Polizeipräsident in seiner Stellungnahme.

Geplant ist ein riesiges „Datenhaus der deutschen Polizei"

So sollen etwa personenbezogene Daten gesammelt und verdichtet werden, um dann Analysen durchzuführen, welche Personen zukünftig welche Straftaten begehen könnten, schreibt Polizeipräsident Norbert Rupp und verweist auf das Programm *Polizei 2020*. Voraussetzung für solche Prognosen über vermeintlich gefährliche Personen sind umfangreiche und leicht durchsuchbare Datenbestände.

Das geplante Gesetz schafft die Grundlage dafür: Die Polizei dürfte damit personenbezogene Daten über Jahrzehnte speichern, denn bei jedem neuen Eintrag zu einer Person würden alle bisherigen Einträge mitgezogen. Die Polizeigewerkschaft (BDK) freut sich, in ihrer Stellungnahme schreibt sie, dass so „kriminelle Karrieren" leicht abgebildet werden können.

Die Landesdatenschutzbeauftragte kritisiert die geplante „Mitzieh-Regel" in ihrer Stellungnahme hingegen als zu pauschal und deswegen unverhältnismäßig:

> *Im Einzelfall kann das dazu führen, dass es bei Personen, die beispielsweise im jugendlichen Alter von 15 Jahren einmalig straffällig werden (z. B. wegen Cannabiskonsum) und die danach nur einmal im Jahrzehnt auffällig werden, sei es durch einen Geschwindigkeitsverstoß oder eine andere Bagatelle, bis zu deren Tod nicht ein einziges Mal zu einer Überprüfung [der erforderlichen Speicherdauer] kommt und der Datensatz über das jugendliche Bagatelldelikt zeitlebens mitgeführt wird.*

66 Bodycams, aber nur zum Schutz von PolizistInnen

In einem anderem Punkt ist die Polizei dem Gesetzgeber schon ein Stück voraus: Bereits heute besitzt die saarländische Polizei insgesamt 66 Bodycams, heißt es aus dem Innenministerium auf Nachfrage von netzpolitik.org. Nun soll eine eigene gesetzliche Grundlage für ihren Einsatz geschaffen werden, es fehlen jedoch eindeutige Regelungen zum Pre-Recording genauso wie ein Verweis auf den Kernbereichsschutz.

Fünf Dockingstationen mit jeweils sechs Body Cams auf einem Schreibtisch – Foto: Sanderflight, CC BY-SA 4.0

Laut Gesetzentwurf dient die Bodycam dazu, Angriffe auf BeamtInnen vorzubeugen. Ein Recht für Betroffene von Polizeigewalt, das Videomaterial einzusehen, ist hier nicht vorgesehen. Dabei weisen Kriminologen darauf hin, dass Gewalt nur interaktiv begriffen werden kann und Bodycams deshalb auch dazu genutzt werden sollten, polizeiliches Fehlverhalten zu dokumentieren[7]. In NRW beispielsweise ist das bereits umgesetzt.

Wer verdächtigt wird zukünftig eine Straftat zu begehen, ist kein „Täter"

Neu eingeführt werden soll zudem die Überwachung mittels elektronischer Fußfessel. In ihrem Koalitionsvertrag schreiben CDU und SPD, dass die elektronische Fußfessel „zur Überwa-

chung von Tätern im Bereich Terrorismus“ dienen soll[8]. Das stimmt so nicht.

Tatsächlich sollen keine Täter überwacht werden, sondern Personen, bei denen die polizeiliche Analyse ergeben hat, dass sie ein hohes Risiko besitzen, in Zukunft eine Straftat zu begehen. Die Überwachung mittels elektronischer Fußfessel ist langfristig konzipiert: Sie beginnt bei drei Monaten und ist danach stets verlängerbar.

Der Nutzen der Maßnahmen ist äußerst zweifelhaft. Zur Verhinderung von terroristischen Straftaten ist die elektronische Fußfessel völlig ungeeignet, da Attentate ihrer Sache nach besonders oft an alltäglichen und viel besuchten Orten stattfinden. Das bestätigt auch ein Vertreter der Gewerkschaft der Polizei (GdP) in der Anhörung.

Laut Polizeigewerkschafter soll die elektronische Fußfessel dazu dienen, „gewaltbereite Fußballfans“ im Schach zu halten. Die Technik sei aber durchaus „diskussionswürdig“ und hätte auch Nachteile, ergänzt ein Vertreter der Deutschen Polizeigewerkschaft (DPolG).

Ausbau der Videoüberwachung in der Innenstadt von Saarbrücken

Derzeit werden Personen, die sich rund um die Johanneskirche in Saarbrücken aufhalten, von der Polizei abgefilmt[9], demnächst beginnt die anlasslose Videoüberwachung auch am Hauptbahnhof.

Mit dem geplanten Polizeigesetz könnten zukünftig weitere Bahnhöfe und Plätze rund um die Uhr abgefilmt werden, mit der Begründung, dass an Orten „dieser Art“ wiederholt Drogen verkauft wurden. Bei Veranstaltungen würde die Annahme genügen, dass Ordnungswidrigkeiten begangen werden könnten, um zu filmen. Die Landesregierung will damit das „subjektive Sicherheitsgefühl“ stärken[10] und die objektive Sicherheitslage verbessern. Tatsächlich sind objektive Effekte der Videoüberwachung auf Kriminalität nicht wissenschaftlich belegt[11]. Punktuelle Videoüberwachung führt vielmehr zu Verdrängung von Kriminalität als zu ihrer Vorbeugung.

Aktions-Bündnis gegen Ausbau polizeilicher Befugnisse

Die Polizeigewerkschaften haben bereits weitere Wünsche beim Innenministerium eingereicht. In einem zweiten Schritt soll demnächst der Präventivgewahrsam gesetzlich erlaubt werden. Damit können Personen, die keine Straftat begangen haben, aber von der Polizei als gefährlich eingeschätzt werden, zeitweise festgehalten werden. In Bayern gibt es eine solche Regelung bereits, dort wurden letztes Jahr ein paar Dutzend Personen wochenlang präventiv eingesperrt[12].

Ende April hat sich im Saarland ein Aktionsbündnis gegen die Verschärfung des Polizeigesetzes[13] gegründet. Gegen die Pläne der schwarz-roten Landesregierung stellen sich die Jugendorganisationen von SPD, Linken, Grünen und FDP, sowie die Linksfraktion im Landtag. Außerdem die saarländische Piratenpartei und die Bündnisse *Seebrücke* und *Omas gegen Rechts*.

Am 28. Mai wird die zweite Anhörung stattfinden. Ob die geplanten technischen Hilfsmittel sinnvoll und notwendig sind, das werden die Landtagsabgeordneten entscheiden. Sie sollten sich dabei nicht nur auf die rechtliche Zulässigkeit berufen.

Quelle: https://netzpolitik.org/2020/neue-ueberwachungswerkzeuge-fuer-die-saarlaendische-polizei/

Anmerkungen

1 *https://www.landtag-saar.de/Downloadfile.ashx?FileId=12915&FileName=Gs16_1180.pdf*
2 *https://cdn.netzpolitik.org/wp-upload/2020/05/Stn_Netzpolitik-Broeckling_SPolDVG-E.pdf*
3 *https://netzpolitik.org/2016/ueberwachungskritisches-urteil-zum-bka-gesetz-und-zum-staatstrojaner/*
4 *https://netzpolitik.org/2018/bayerisches-polizeigesetz-billige-tricks-der-csu-entlarvt/*
5 *https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html*
6 *https://www.landtag-saar.de/Downloadfile.ashx?FileId=12915&FileName=Gs16_1180.pdf*
7 *https://netzpolitik.org/2017/lass-dich-ueberwachen-die-neue-informationelle-sozialpflichtigkeit/*
8 *https://www.cdu-fraktion-saar.de/cdusaar/uploads/2017/09/Koalitionsvertrag_CDU_SPD_2017-2022_final4.pdf*
9 *https://www.saarland.de/249526.htm*
10 *https://www.saarland.de/dokumente/res_stk/Halbzeitbilanz_2019_Inhverz.pdf*
11 *https://kfn.de/wp-content/uploads/Forschungsberichte/FB_143.pdf*
12 *https://netzpolitik.org/2019/bayerisches-polizeigesetz-19-personen-wochenlang-in-praeventivgewahrsam/#spendenleiste*
13 *https://www.sr.de/sr/home/nachrichten/politik_wirtschaft/buendnis_gegen_neues_polizeigesetz_100.html*
14 *https://pgp.mit.edu/pks/lookup?op=get&search=0xC0439F206973E506*

Marie Bröckling

Marie Bröckling arbeitet seit Februar 2018 für *netzpolitik.org*. Sie schreibt und spricht vor allem über die Polizei, zum Beispiel auf der *re:publica* und auf dem *Chaos Communication Congress*. Sie ist unter *marie.broeckling (at) netzpolitik.org* (PGP-Key[14]) erreichbar und als *broeckling_* auf Twitter.

Anna Biselli

Geflüchtete klagen gegen das Auslesen ihrer Handys

Wer in Deutschland Asyl sucht und keinen Pass vorlegen kann, muss damit rechnen, dass sein Smartphone ausgelesen wird. Gegen diesen Eingriff ziehen nun Geflüchtete vor Gericht. Die Praxis betrifft Tausende Geflüchtete pro Jahr.

Seit fast drei Jahren darf das Bundesamt für Migration und Flüchtlinge (BAMF) die Smartphones Asylsuchender auswerten[1], die sich ohne Pass in Deutschland um Asyl bewerben. Schon als das Gesetz erarbeitet wurde, wurde die Verhältnismäßigkeit der Datenauslesung angezweifelt – unter anderem von der damaligen Bundesdatenschutzbeauftragten[2]. Nun klagen drei Betroffene[3] vor Verwaltungsgerichten in Berlin, Hannover und Stuttgart gegen die Praxis. Unterstützt werden sie von der Gesellschaft für Freiheitsrechte.

Einer der Kläger ist der 29-jährige Mohammad A., der aus Syrien nach Deutschland geflohen war. Auch sein Handy wurde ausgelesen. Warum, konnte er nicht verstehen – er war schon längst als Geflüchteter in Deutschland anerkannt. „Ich wusste überhaupt nicht, was da genau passiert, man hat mir nichts erklärt. Aber ich hatte Angst, abgeschoben zu werden. Also habe ich ihm das Handy gegeben. Das war, als würde ich mein ganzes Leben über den Tisch reichen", sagt er laut Pressemitteilung[4]. An seinem Asylstatus änderte die Nachüberprüfung im Jahr 2019 nichts. Die beiden weiteren Klägerinnen sind eine 37-jährige Frau aus Afghanistan und eine 25-Jährige aus Kamerun.

Die Migrationsbehörde wertet die Geräte aus, um Hinweise auf Herkunft und Identität der Asylsuchenden zu bekommen. Zweifel an ihren Angaben sind dafür nicht Voraussetzung, die Datenträgerauslesung kommt schon in Betracht, wenn eine Person keinen gültigen Pass vorzeigen kann. Es muss nicht versucht werden, die Herkunftsangaben durch weniger invasive Mittel wie eine Asylanhörung zu überprüfen.

Bei der Analyse werden etwa die Ländercodes ein- und ausgehender Nachrichten und Anrufe, Geodaten sowie die verwendete Sprache bei Textnachrichten untersucht. Dann steht da beispielsweise: 64 Prozent der getätigten Anrufe des Antragstellers gehen zu Telefonnummern mit tunesischer Vorwahl. 52 Prozent der eingehenden Textnachrichten sind in französischer Sprache verfasst. Aber auch Profilnamen werden ausgewertet, etwa von Google- oder Facebook-Accounts, die auf dem Gerät gefunden werden.

Oftmals bringt die Auswertung keine brauchbaren Ergebnisse

Letztes Jahr hat das Bundesamt 10.116 Datenträger von Erstantragstellern ausgelesen[5]. Etwa 4.600 Mal beantragten Entscheider Zugriff auf diese Auswertungen, davon wurden bis April 2020 etwa 3.400 durch einen Volljuristen freigegeben. Oft bringen diese Auswertungen nichts: 2019 habe es in 58 Prozent der Fälle keine verwertbaren Ergebnisse gegeben, bei 40 Prozent hätte sich die Identität der Antragstellenden bestätigt, in nur zwei Prozent sei sie widerlegt worden.

Die wenigen verwertbaren Ergebnisse lassen zweifeln, ob das Verfahren überhaupt geeignet ist, Anhaltspunkte für Identität und Herkunft zu bekommen. Dafür greift es tief in die Privatsphäre Geflüchteter ein, die sich in einem starken Abhängigkeitsverhältnis zu dem Land befinden, in dem sie Asyl suchen – und sich deshalb kaum gegen den Eingriff verwehren können.

„Das BAMF missachtet die hohen verfassungsrechtlichen Vorgaben, an die der Staat beim Zugriff auf persönliche Daten gebunden ist", sagt Lea Beckmann, Juristin bei der GFF. Sie koordiniert das Verfahren, bei dem es nicht nur um die drei aktuell Klagenden geht, sondern um Tausende Geflüchtete, die ihre Datenträger herausgeben mussten. Und so soll auch beim Verwaltungsgericht nicht Schluss sein[6]: „Ziel ist, die gesetzliche Grundlage für die Handydatenauswertung vor das Bundesverfassungsgericht zu bringen."

Offenlegung: Die Autorin dieses Artikels hat als Co-Autorin an der Studie „Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa" mitgewirkt, die die GFF in Vorbereitung auf die Klageverfahren erstellte.

Quelle: https://netzpolitik.org/2020/gefluechtete-klagen-gegen-das-auslesen-ihrer-handys/

Anmerkungen

1 *https://netzpolitik.org/2017/jetzt-doch-behoerde-will-auch-geodaten-aus-handys-von-gefluechteten-auswerten/*
2 *https://www.zeit.de/politik/deutschland/2017-03/fluechtlinge-andrea-vosshoff-handydaten-identitaetspruefung-kritik-datenschutz-bundesregierung*
3 *https://freiheitsrechte.org/refugee-daten/*
4 *https://freiheitsrechte.org/pm-klagen-handyauswertung/*
5 *http://dipbt.bundestag.de/dip21/btd/19/184/1918498.pdf*
6 *https://freiheitsrechte.org/refugee-daten/*
7 *https://keys.openpgp.org/search?q=anna@netzpolitik.org*

Anna Biselli

Auf einem Zettel steht, dass **Anna Biselli** eigentlich Informatikerin ist. Sie ist seit 2013 bei *netzpolitik.org* dabei. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund ums BAMF. Du erreichst sie unter *anna@netzpolitik.org* – am besten verschlüsselt [325C 6992 DCD3 1167 D9FA 9A57 1873 5033 A249 AE26][7]

Wolf Schünemann

Desinformation zu bestrafen, ist die falsche Therapie

Zur Pandemie kommt die sogenannte Infodemie. Weltweit reagieren Staaten auf die Verbreitung vermeintlicher Falschnachrichten. Doch wer legt fest, was richtig und falsch ist? Der Fall des chinesischen Arztes Li Wenliang ist dabei ein mahnendes Beispiel. Ein Kommentar.

Die sorgenvollen Debatten über das neue Coronavirus COVID-19 werden aktuell von der Angst vor Falschinformationen, „Fake News", begleitet. So wie sich mehr und mehr Menschen auf der ganzen Welt mit dem Virus infizieren und daran erkranken, drohen sich auch Gerüchte und falsche Behauptungen zum Ursprung, zu geeigneten Behandlungsmaßnahmen oder gebotenen Bewältigungsstrategien, ebenso wie allerlei haarsträubende Verschwörungstheorien, auszubreiten.

Die Weltgesundheitsorganisation WHO spricht von einer „Infodemie"[1], die mit der globalen Pandemie einhergehen und ihre Folgen womöglich erschweren würde. Weltweit reagieren Staaten auf diese wahrgenommene Bedrohung, indem sie teils drakonische Strafen für die Verbreitung von „Gerüchten" und Falschnachrichten verhängen und die Pressefreiheit einschränken.

Verschärfte Maßnahmen gegen Corona-Fake-News

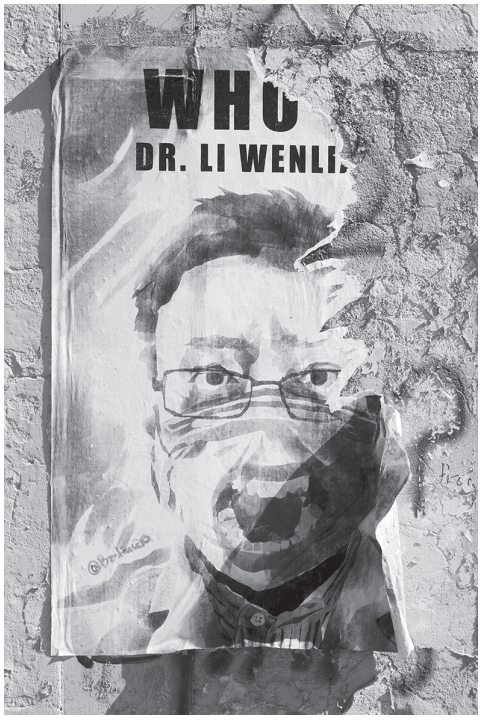
Vor wenigen Tagen eröffnete die Organisation *Reporter ohne Grenzen* eine Themenseite zur Pandemie[2], auf der sie die staatlichen Eingriffe dokumentiert. Auch hierzulande haben führende Innenpolitiker auf Landes- und Bundesebene angekündigt, mit verschärften Maßnahmen gegen Fake News in Corona-Zeiten vorgehen zu wollen.

Wie der Sprecher des Bundesinnenministeriums Kerber dem Handelsblatt mitteilte[3], setzt die Bundesregierung dabei auf die führenden Internetunternehmen und Plattformbetreiber, die ihre Anstrengungen im Kampf gegen Falschinformationen in Koordination mit der Politik steigern müssten. Er stellt in diesem Zusammenhang aber auch zusätzliche staatliche Eingriffe in Aussicht.

Der niedersächsische Innenminister Boris Pistorius war in der vergangenen Woche noch weiter gegangen. Medienberichten zufolge forderte er effektive Sanktionen[4], etwa gegen die Verbreitung von Falschnachrichten zur Pandemie oder zur öffentlichen Versorgungslage und brachte damit eine Strafrechtsreform ins Spiel.

Vieles spricht dafür, dass die Coronakrise und die begleitende sogenannte „Infodemie" Deutschland und andere westliche Demokratien einen Pfad weiter beschreiten lassen werden, der in vielen Ländern und auch auf europäischer Ebene bereits vor der Krise erkennbar angelegt war: denjenigen der institutionalisierten und womöglich gar strafbewehrten Bekämpfung von Desinformation im Netz.

Frankreich hat dazu mit Blick auf den Wahlkampf bereits 2018 ein Gesetz erlassen. Deutschland selbst hat mit dem Netzwerkdurchsetzungsgesetz ein international viel beachtetes Äquivalent im Kampf gegen Hassrede und Hetze geschaffen, in dessen Rechtfertigung Hass und Desinformation oft als gemeinsame Bedrohung vorgetragen wurden. Die Bekämpfung von Desinformation ist als Ziel staatlicher Online-Kontrollmaßnahmen also ins Visier der Politik genommen.



Partially damaged picture of Dr. Li Wenliang on the wall poster – Petr Vodička, CC BY-SA 4.0

Was Desinformation ist, kann nur mit Abstand geklärt werden

Forderungen in diese Richtung erhalten in Zeiten der Krise, die ohnehin eine Stunde der Exekutive ist, erheblichen Auftrieb. Anders als Hassrede und Hetze aber, die sich anhand sprachlicher und situativer Merkmale noch einigermaßen sicher, vielleicht gar objektiv, feststellen lassen (aktuelle Beispiele wie der Fall von Renate Künast[5] zeigen auch hier bereits die Grenzfälle), sind vergleichbare klare Maßstäbe bei der Desinformation nicht gegeben.

Ob etwas Desinformation ist, ob etwas ein bloßes Gerücht oder eine Falschbehauptung darstellt oder möglicherweise doch die Wahrheit und ein Beitrag zur Aufklärung ist, ist in vielen Fällen eine ausgesprochen komplexe Entscheidung. In Zeiten, in denen sich die Faktenlage dynamisch verändert, kann sie nur mit Abstand überhaupt geklärt werden. Im Augenblick der Verbreitung fehlt oft der Maßstab.

Selbst wenn die Verschwörungstheorie abstrus, die Lüge offensichtlich ist, die abschreckende Wirkung von Strafmaßnahmen gegen ihre Verbreitung, droht echte Aufklärerinnen und Investigativjournalisten zur Zurückhaltung, womöglich zur Selbstzensur, und Betreiber digitaler Plattformen zu Überreaktionen bei der Inhalteregulierung (Overblocking) zu zwingen. Damit wird die Bekämpfung von Desinformation zu einer zweifelhaften, ja bedrohlichen Therapie in einem demokratischen Gemeinwesen.

Der Fall Li Wenliang ist eine Mahnung

Daran gemahnt, abgesehen von den vielfach dokumentierten Eingriffen etwa auf der Seite von Reporter ohne Grenzen, ein besonders prominenter Fall von Einschränkung der Informationsfreiheit in der chinesischen Volksrepublik, ohnehin einem Vorreiterland und abschreckenden Beispiel, wenn es um Eingriffe in die Presse- und Internetfreiheit[6] geht: der Fall Li Wenliang.

Dass dieser hinsichtlich des unterstellten Delikts und der Strafe für das Land keineswegs außergewöhnliche Fall überhaupt eine internationale Aufmerksamkeit erfahren hat, hängt mit der globalen Corona-Epidemie zusammen. Denn es war der junge Mediziner Li, der als einer der ersten vor der neuartigen Krankheit warnte und einige Wochen später infolge der eigenen Infektion mit dem Virus verstarb.

Li hatte den umstrittenen Post von seiner Entdeckung selbst nur innerhalb eines geschützten Bereichs auf der Plattform WeChat versendet, und dies zunächst in einer verkürzten Form, wonach sieben Personen in Wuhan positiv auf das SARS-Virus getestet worden seien. Unbekannte Teilnehmer des Gruppenchats verbreiteten Screenshots dieser alarmierenden Mitteilung[7] über öffentliche Kanäle, ohne von Li wenig später gepostete Erklärungen hinzuzufügen, wonach es sich um ein verwandtes Corona-Virus unbekannten Typs handle.

Daraufhin wurde Li von der regionalen Sicherheitsbehörde in Wuhan vorgeladen. Mit seiner Mitteilung hatte er gegen das Gesetz verstoßen. Ihm wurde offiziell zur Last gelegt, er habe „online Gerüchte verbreitet" und dadurch die „soziale Ordnung schwer gestört". Li wurde mittels Strafandrohung dazu gezwungen, seine Mitteilung schriftlich zu widerrufen.

In der Bewertung der Folgen des Falls muss man nicht so weit gehen, wie die NGO Reporter ohne Grenzen, wenn sie spekuliert, dass das Coronavirus mit Medienfreiheit in China womöglich nicht zur globalen Pandemie geworden wäre[8]. Der Fall Li Wenliang illustriert ohnedies aber: Die Bekämpfung sogenannter Falschnachrichten und Gerüchte durch staatliche Behörden kann katastrophale Folgen haben, etwa wenn die rasche Aufklärung von Gesundheitsrisiken oder auch die Arbeit von Investigativjournalisten verhindert wird. Gravierender noch als die Sanktionierung im Einzelfall kann sich die durch die Sanktionspraxis bewirkte Abschreckung und Selbstzensur als eine Gefährdung der demokratischen Öffentlichkeit auswirken.

Somit stellt schon die Existenz einer gesetzlichen Regelung ein Problem dar. Im konkreten Fall haben die chinesischen Behörden nicht das Recht gebeugt, sie haben es nicht missbraucht, sondern das geltende Recht schlicht angewendet. Dr. Li hatte unter den damaligen Bedingungen in seinem ersten Post ein Gerücht verbreitet. Noch dazu hat er sich zu diesem frühen Zeitpunkt, zu dem der Typ des Virus noch nicht feststand, bei seiner tentativen Bestimmung geirrt.

Wer legt fest, was richtig oder falsch ist?

Der Fall verdeutlicht zudem, dass die Bestimmung von Desinformation zu unsicher ist, um darauf ein Gesetz aufzubauen. Wer sollte in jeder Situation autoritativ festlegen können, was richtig und was falsch ist? Was sollte bei einer dynamischen Informationslage der richtige Maßstab sein, die Faktenlage, also der aktuelle Kenntnisstand, politische Opportunitäten? Wie steht es um die Verbindlichkeit und die Haltbarkeit von derlei Setzungen?

Auf diese Fragen gibt es – zumindest in einer liberalen Demokratie – keine überzeugende Antwort. Damit sollen keine abstrusen Verschwörungstheorien und abwegigen Erklärungen veredelt oder pauschal entschuldigt werden. Wie bei so viel Fragen, bei denen wir derzeit den Gesetzgeber anrufen, scheint die Ethik, die gesellschaftliche Konstruktion von und die Erinnerung an gesellschaftliche Normen auch hier der geeignetere Weg.

Gerade in diesen außergewöhnlichen Zeiten, in denen Grundrechte im Zeichen des öffentlichen Gesundheitsschutzes empfindlich eingeschränkt werden, weit über das Maß hinaus, das wir uns noch vor Wochen als für liberale Demokratien geboten vorgestellt haben, müssen wir auf die Verhältnismäßigkeit der eingesetzten Mittel achten. Die Bekämpfung von Desinformation allerdings kennt kein vernünftiges Maß.

Die heute zur Rechtfertigung skizzierten potenziellen Folgen von Falschbehauptungen – die angebliche Anfachung sozialer Konflikte, die Steigerung einer diffusen Panik, im konkreten Fall: noch mehr Hamsterkäufe – sie allesamt sind auch unabhängig

Wolf Schünemann

Wolf Schünemann ist Juniorprofessor für Politikwissenschaft mit dem Schwerpunkt Politik und Internet an der Universität Hildesheim. Seine Forschungsschwerpunkte liegen in den Bereichen digitalpolitischer Regulierung, politischer Online-Kommunikation und Politik im europäischen Mehrebenensystem. Methodisch arbeitet er vor allem an und mit Verfahren der Diskursanalyse, einschließlich qualitativer, quantitativer und automatisierter Analysetechniken. Bei den Recherchen zu diesem Beitrag wurde er von Wanchen Wang, Promotionsstudentin an der Universität Hildesheim, unterstützt.

von Falschnachrichten keineswegs ausgeschlossen und ergeben keine hinreichende Begründung für so grundlegende Eingriffe in die Meinungs- und Informationsfreiheit mit potenziell weit gravierenderen Folgen für die Demokratie.

Herdenimmunität im Kampf gegen die Infodemie

Die liberale Demokratie zeichnet sich nicht dadurch aus, dass das System oder der sogenannte soziale Frieden vor der freien Rede geschützt werden, sondern umgekehrt: die freie Rede vor den Eingriffen des Systems. Das Ziel, diese freie Rede auf der anderen Seite auch vor sich selbst und insbesondere vor möglicherweise gezielten manipulativen Eingriffen neuer Art zu bewahren, muss dabei nicht verkehrt sein.

Aufmerksamkeitskampagnen, Faktenchecks und redaktionelle Qualitätskontrolle auch durch Plattformbetreiber könnten hier sinnvolle Maßnahmen sein. Wie zum Schutz der Gesundheit ist auch auf eine individuelle Hygiene zu achten, etwa was das Online-Suchverhalten, die abonnierten Newsfeeds und die sozialen Netzwerke angeht. Staatliche Eingriffe in die Informationsfreiheit im Netz aber, begründet durch eine autoritativ geltende Wahrheit oder etwas niederschwelliger: Faktenlage, wie in Autokratien praktiziert, ist hingegen eine schädliche Therapie.

Wir alle sollten stattdessen an unserer digital-informationellen Mündigkeit arbeiten und den gesunden Menschenverstand zur Abwehr von Falschbehauptungen, abstrusen Gerüchten und Verschwörungstheorien mobilisieren. Zumindest im Kampf gegen die Infodemie scheint die Herdenimmunität damit die bessere Strategie zu sein als die Suppression.

Quelle: https://netzpolitik.org/2020/desinformation-zu-bestrafen-ist-die-falsche-therapie/

Anmerkungen

1 *http://www.euro.who.int/de/about-us/regional-director/speeches-and-presentations-by-year/2020/address-at-the-employment,-social-policy,-health-and-consumer-affairs-council,-european-council*
2 *https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/rsf-startet-themenseite-zur-pandemie/*
3 *https://www.handelsblatt.com/politik/international/falschinformationen-berlin-und-bruessel-kaempfen-gegen-die-infodemie/25672130.html*
4 *https://www.spiegel.de/politik/deutschland/coronavirus-boris-pistorius-fordert-strafen-gegen-fake-news-a-ed5050b5-c194-4890-a4c3-c713290134f3*
5 *https://netzpolitik.org/2020/dieses-urteil-ist-ein-gutes-zeichen/*
6 *https://freedomhouse.org/report/freedom-net.*
7 *https://www.cnn.com/2020/02/08/opinions/coronavirus-bociurkiw/index.html*
8 *https://rsf.org/en/news/if-chinese-press-were-free-coronavirus-might-not-be-pandemic-argues-rsf*

FIfF e. V.

Wissenschaftlicher Beirat des FIfF

Das FIfF hat zur Beratung in wissenschaftlichen und satzungsmäßigen Fragen einen Beirat eingerichtet. In den Beirat lädt der Vorstand Persönlichkeiten ein, die für das Fachgebiet *Informatik und Gesellschaft*, dessen wissenschaftliche Bearbeitung und die sich in diesem Umfeld ergebenden gesellschaftspolitischen Fragen eine herausragende Rolle spielen.

Der Vorstand des FIfF hat in seiner Sitzung am 1./2. Februar 2020 in Weimar beschlossen, drei neue Mitglieder in den Beirat zu berufen:

Lange Zeit war Professor Dr. **Dietrich Meyer-Ebrecht** Mitglied im Vorstand des FIfF und dessen stellvertretender Vorsitzender. Dabei hat er wesentliche Beiträge zum Inhalt und zur Organisation des FIfF geleistet. Er ist die treibende Kraft hinter dem Projekt TDRM, das auch über das FIfF hinaus große Beachtung gefunden hat und findet. Auch darüber hinaus hat er wertvolle inhaltliche Beiträge geleistet, unter anderem zum Thema Rüstung und Informatik in der Kampagne *Cyberpeace*, als Vertreter des FIfF bei vielen Konferenzen und durch viele Beiträge zur FIfF-Kommunikation und zu anderen Publikationen. Lange Zeit hat er das FIfF auch im Vorstand des Trägervereins der Zeitschrift *Wissenschaft & Frieden* vertreten und ist heute noch Mitglied in dessen Beirat. Dazu kommt die unschätzbare organisatorische Arbeit, die er für das FIfF geleistet hat.

In seiner sechsjährigen Zeit im Vorstand hat auch Professor Dr. **Eberhard Zehendner** wesentliche Beiträge zur Arbeit des FIfF geleistet. Neben seiner Arbeit an der FIfF-Kommunikation, wo er sowohl in der Hauptredaktion aktiv war als auch mehrere Schwerpunkthefte – zweimal zum Datenschutz, zu Cybercrime und das Konferenzheft TRUST – gestaltet hat, war er der Organisator einer großartigen Konferenz in Jena. Wir freuen uns, dass wir auch in diesem Jahr auf seine Mitarbeit zählen können.

In seiner vierjährigen Mitgliedschaft im Vorstand hat **Benjamin Kees** ebenfalls wichtige Beiträge zur Arbeit des FIfF geleistet. Er war an der Organisation großartiger Tagungen in Berlin beteiligt. 2014 konnten wir ihm für seine Diplomarbeit den FIfF-Studienpreis, den heutigen Weizenbaum-Studienpreis, verleihen, für eine Arbeit auf dem Gebiet der automatisierten Videoüberwachung – einem der Kernthemen des FIfF. Er ist auch treibende Kraft bei den Aktivitäten zum *Verunsicherungsbahnhof* Berlin Südkreuz. Zusätzlich hat er viel dafür getan, unsere IT voranzubringen.

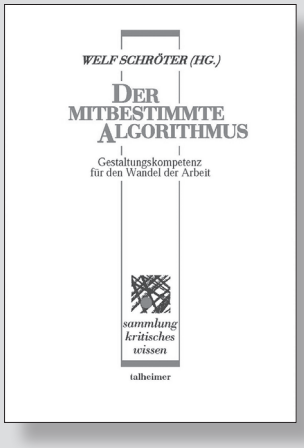
Dietrich, Eberhard, Ben, wir begrüßen Euch im Beirat des FIfF und freuen uns auf die weitere Zusammenarbeit.

Dagmar Boedicker

Welf Schröter Hg.: „Der mitbestimmte Algorithmus“

In neun Aufsätzen stellen die Autorinnen und Autoren Kriterien für die zulässige Implementierung einer Technik vor, „die den Anspruch erhebt, an Stelle des Menschen rechtsverbindliche Entscheidungen in Echtzeit zu treffen.“[1] *Heutige KI beschreiben sie als weitere Entwicklung hin zu Systemen, die statistische Information aus Daten ziehen und Muster erkennen, die mit Robotik verschmelzen können, Prozesse simulieren und steuern, Ergebnisse vorhersagen und möglicherweise Entscheidungen von Menschen ersetzen. Wo KI eingesetzt wird, hänge davon ab, ob eine Steuerung mehr Rationalisierung möglich macht, ob das weniger koste als die menschliche Arbeitskraft und welche Bereiche in welchem Ausmaß modellierbar und programmierbar seien. Die Systeme seien intransparent und es tue sich eine mögliche Verantwortungslücke auf. Mit 30 handhabbaren Kriterien zum Umgang richtet sich das Buch vor allem an die Vertretungen der Beschäftigten.*

Im ersten Beitrag analysiert *Klaus Kornwachs,* wie KI das Verhältnis zwischen den Eigentümern der Produktionsmittel und der Gesellschaft verändert und die Machtverhältnisse verschiebt. Er betrachtet die Rollen von arbeitenden und konsumierenden Menschen, deren Freiheit zu wählen schrumpft durch Automatisierung, zunehmende Kundenbindung und Abhängigkeit, die sich kümmerliche Anerkennung durch Wohlverhalten erkaufen müssen und deren Produktivkraft sich im bröckelnden Sozialstaat sanktionslos abschöpfen lässt.



Welf Schröter (Hg)
Forum soziale Technikgestaltung
Der mitbestimmte Algorithmus
Gestaltungskompetenz für den Wandel der Arbeit
Talheimer Verlag, Mössingen
Klappenbroschur, 242 Seiten
Preis: 39,00 Euro
ISBN: 978-3-89376-181-4

Oleg Cernavin setzt sich mit verschiedenen KI-Begriffen auseinander – er spricht von *intelligenter Software (inkl. KI) –,* um die Debatte vor allem in der Arbeitswelt zu erleichtern. Er unterscheidet zwischen technischer und menschlicher Autonomie, fordert dazu auf, die Intentionen derer zu prüfen, die KI anbieten, sich die grundlegende Funktionsweise und den Umgang mit den personenbezogenen Daten klar zu machen, genau nachzusehen, welche Arbeitsprozesse sich wie verändern und wie die Unternehmens*kultur* dazu passt, und was KI mit Intuition und Erfahrungswissen der Menschen anstellt. Am Ende des gut strukturierten und verständlichen Beitrags listet Cernavin wichtige Kompetenzen der Beschäftigten in Zukunft auf und skizziert Umsetzungshilfen und eine Potenzialanalyse, die online verfügbar sind.

Jan Etscheid und *Jörn von Lucke* haben für den öffentlichen Bereich die *Anwendungs*sicht auf KI gewählt und betrachten die Design-Anforderungen aus der Perspektive der jeweils Betroffenen als Beschäftigte, Politik, Bürgerinnen und Bürger. Dabei hat mich gewundert, dass sie die Datenschutz-Grundverordnung nicht erwähnen. Deren Art. 22 zum Thema automatisierte Entscheidungen lässt zwar Ausnahmen vom Verbot im nationalen Recht zu (Öffnungsklausel), darüber hätte ich aber gern mehr erfahren.

Schließlich liegt genau hier das Problem –, in dem, was *Welf Schröter* in seinem Beitrag als *Delegationstechnik* bezeichnet. Autonome Software-Systeme (ASS) entscheiden in der Produktion, der Verwaltung, über Beschäftigte, Bürger und Kunden. Sie „steuern die Arbeit und den Menschen“,[2] ein Paradigmenwechsel nach der bisherigen „Handlungsträgerschaft Mensch“[3]. Welf Schröter gibt Positionen einiger Gruppen wieder, die sich bisher im Sinne des titelgebenden Konzepts *mitbestimmter Algorithmus* geäußert haben: AlgorithmWatch, Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz der EU, Gesellschaft für Informatik, Konferenz der unabhängigen Datenschutzaufsichtsbehörde des Bundes und der Länder, Bertelsmann Stiftung, Unternehmensnetzwerk D21, Verbraucherzentrale Bundesverband.[4] An diesen Positionen bemängelt er zu Recht eine geringe oder fehlende Mitbestimmungs-Perspektive. Damit die Mitbestimmung der KI-Herausforderung begegnen kann, schlägt Schröter eine vierte Ebene zu den bisherigen (Gesetze, Tarifverträge, betriebliche Vereinbarungen) vor. Sie soll die von ihm ausgemachten *strukturellen Grenzüberschreitungen*, getrieben von zwölf Faktoren[5], zähmen und Folgendes erarbeiten: Orientierungswissen, vorausschauende Arbeitsgestaltung, generische Kriterien für die Freigabe von ASS, Voraussetzungen für die Mitarbeit an Spezifikationen und Partizipation, Betriebs-/Dienstvereinbarungen zur Beteiligung, zu den Einsatzgebieten und Eigenschaften der Systeme. Das sollten nach Ansicht des *Forums soziale Technikgestaltung* Betriebsräte und Gewerkschaften anstreben.

Ein Abschnitt des Buchs befasst sich mit Crowd Work in seinen aktuellen Formen und im letzten Abschnitt finden sich eine Konzernbetriebsvereinbarung zum *internen Crowdsourcing* und der Entwurf einer Rahmen- und Zukunfts-Dienstvereinbarung IT und TK, erstere *lebend,* die zweite *lernend.*

Gut gefallen hat mir an dem Buch, dass seinen Autorinnen und Autoren bewusst zu sein scheint, dass die KI-Diskussion seit 40 Jahren stattfindet und KI als solche nicht überschätzt werden sollte. Es geht um Technikgestaltung, heute wie damals. In ihrer aktuellen Erscheinungsform ist IKT eben nicht menschenzentriert, auch nicht ökologisch nachhaltig. Und weil die Machtverhältnisse sind wie sie sind, ist es ein mühseliger Prozess das zu ändern. Viel Erfolg uns allen dabei!

Anmerkungen

1 *Klappentext*
2 *S. 116*
3 *S. 111*
4 *Ich empfehle auch noch die Positionen im Gutachten der Datenethikkommission der Bundesregierung vom Oktober 2019*
5 *S. 132ff*

Dagmar Boedicker

Adrian Lobe: „Speichern und Strafen – die Gesellschaft im Datengefängnis“

Adrian Lobe *hat den Titel gut gewählt. Er spielt damit auf Michel Foucaults „Überwachen und Strafen“ an. Die Machtmaschine ist so perfekt, dass es fast überflüssig wird, Macht tatsächlich anzuwenden. Alle Insassen des* Panoptikons *haben sie verinnerlicht. Endstation dieser Entwicklung könnte eine „post-voting society“ sein, wie sie in einer Broschüre des Bundesinstituts für Bau-, Stadt- und Raumforschung von 2017*[1] *skizziert wird.*

Jedes Speichern ist Arrest: „Man muss Menschen nicht mehr wie im Mittelalter in Kerker und dunkle Verliese stecken. Sie inhaftieren sich selbst.“ (S. 28) Lobe befasst sich in diesem Buch auch mit den Folgen für den Rechtsstaat, wenn er das „Vorverbrechen“ im Rahmen vorausschauender Polizeiarbeit beschreibt: „Der militärisch-industrielle Komplex muss laufend Bürger screenen, damit die metastabile Ordnung aufrechterhalten wird.“ (S. 30) So auch, wenn er kritisiert, dass Algorithmen-basierte Entscheidungen außerhalb der Rechtsordnung wirken, „weil sie gesetzliche Normen suspendieren und in maschineller Dezision eigene Normen erzeugen. Der Algorithmus ist, um mit Agamben zu argumentieren, eine ‚verfassungsmäßige Diktatur', eine autoritäre Normproduktionsmaschine.“ (S. 39f) Kapitel 3 ist untertitelt: „Wer braucht noch Gesetze, wenn es Programmcodes gibt?“

Adrian Lobe:
Speichern und Strafen. Die Gesellschaft im Datengefängnis
C. H.Beck oHG, München
Klappenbroschur, 256 Seiten
Preis: 16,95 Euro
ISBN: 978-3-406-74179-1

Wenn Code aber zum Gesetz wird, dann hat das nichts mehr mit Demokratie zu tun, in der Normen sich aus gesellschaftlichen Verhandlungen ergeben. Dann können technische Voreinstellungen Verstöße unmöglich machen und damit die Norm dem politischen Diskurs entziehen. Dabei sind es gerade häufige Regelverstöße, durch die soziale Probleme erkennbar werden.

Anhand zahlreicher Beispiele dokumentiert der Autor das uns umgebende Panoptikon und die algorithmische Steuerung der Gesellschaft, die wir nur in unserer grenzenlosen Naivität als weit entfernt von chinesischen Verhältnissen betrachten. Soziales Management programmiert die staatliche Sicherheit. Die vielen konkreten Beispiele lesen sich gut, es ist ein interessantes Buch, beunruhigend und gleichzeitig kurzweilig. Für gewohnheitsmäßige Leserinnen und Leser der *FIfF-Kommunikation* sind manche der geschilderten Tatsachen sicher nicht neu, Lobe ordnet aber die Überwachungs-Phänomene in einen philosophischen und demokratie-theoretischen Zusammenhang ein, der das Buch lesenswert macht.

So stellt er fest:

> *„Die von der Gegenkultur der 68er-Bewegung betriebene Dekonstruktion von Disziplinarapparaten führt dazu, dass sich der zunehmend als Selbstdisziplin verstandene Gehorsam ein neues Gehäuse schafft: das Datengefängnis.“ (S. 165)*

Lobe kritisiert scharf die Schablonen der Datenkraken, die sie über die ganze Gesellschaft legen:

> *„Die programmierte Gesellschaft steuert auf einen Punkt zu, an dem Distinktion und damit Differenz zur Illusion werden, weil jeder mit einer Datenuniform herumläuft und in denselben Formeln erzählt wird. Uniformität wird in der programmierten Gesellschaft informationell hergestellt.“ (S. 222)*

Statt sich emanzipiert von elektronischer Aufsicht zu fühlen, fühlen sich die Opfer von *Nomophobie* (No Mobile Phone Phobia) wie in Isolationshaft, in einer Zelle mit Funkloch (S. 167). Mich hat das Buch an Jörg Pohles Artikel in der *FIfF-Kommunikation* 4/2019 erinnert, in dem er eine *Freiheitsbestands-Analyse* vorschlägt: Wir sollten endlich prüfen, an welchen Orten wir überhaupt noch frei von Erfassung, Überwachung und sogar Fremdsteuerung leben.

Anmerkungen

1 *https://www.bbsr.bund.de/BBSR/DE/Veroeffentlichungen/Sonderveroeffentlichungen/2017/smart-city-charta-dl.pdf?__blob=publicationFile&v=2 (abgerufen 16.1.2020)*
2 *Samantha Hoffman: Programming China*

FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder

Mailingliste Videoüberwachung:
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Mitglieder-Wiki
https://wiki.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Kaiserslautern); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Christiane Floyd** (Berlin); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (München); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (München); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (München); **Benjamin Kees** (Berlin); **Ulrich Klotz** (Frankfurt am Main); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr**. Klaus-Peter Löhr** (Berlin); Prof. Dr. **Dietrich Meyer-Ebrecht** (Aachen); **Werner Mühlmann** (Calau); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Paderborn); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Mainz); Prof. Dr. **Eberhard Zehendner** (Jena)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Maximilian Hagner – Jena
Alexander Heim – Berlin
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Prof. Dr. **Werner Winzerling** – Fulda

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Philip Love – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Arne Buß und Werner Winzerling
V.i.S.d.P.	Stefan Hügel
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder, München
Cover	https://commons.wikimedia.org/wiki/File:SARS-CoV-2_without_background.png
Druck	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.

KLIMAneutral produziert

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

Virtuelle FIfF-Konferenz 2020
14.+15. November 2020

FIfF-Kommunikation

3/2020 „IT und Klima/Nachhaltigkeit" (Arbeitstitel)
Dagmar Boedicker u. a.
Redaktionsschluss: 15. Juli 2020

4/2020 „Digitalisierung" (Arbeitstitel)
Stefan Hügel u. a.
Redaktionsschluss: 15. Oktober 2020

Zuletzt erschienen:
1/2019 Brave new World 1
2/2019 Brave new World 2
3/2019 Cyberpeace und IT-Security
4/2019 Überwachungs-Gesamtrechnung
1/2020 Künstliche Intelligenz als Wunderland

W&F – Wissenschaft & Frieden
3/19 Hybrider Krieg?
4/19 Ästhetik im Konflikt
1/20 Atomwaffen – Schrecken ohne Ende?
2/20 Frieden begreifen

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#228 Wohnen als soziales Grundrecht
#229 Sterbehilfe
#230 30 Jahre Deutsch-Deutsche Wiedervereinigung
#231 Drei Jahre Praxiserfahrung – Evaluation der DSGVO
#232 Berliner Gespräche – Staat, Religion und Weltanschauung
#233 Informationsfreiheit

DANA – Datenschutz-Nachrichten
1/20 Gesundheitsdaten – Geheim oder Gemeingut?
2/20 E-Payment
3/20 E-Government – Datenschutz in öffentlichen Stellen
4/20 Mobilität

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
Philip Love
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Schluss FIfF

FIfF e. V.

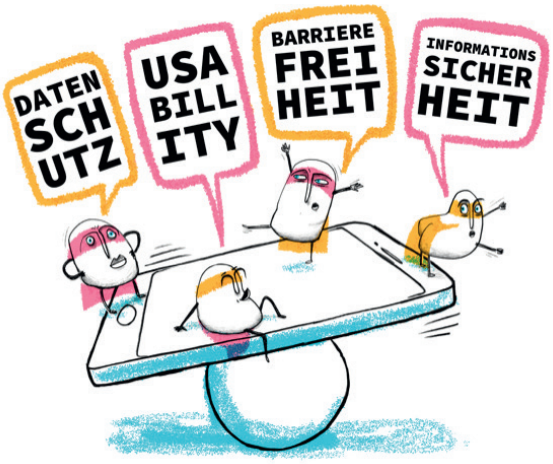
Corona und das FIfF

Es ist nicht zu übersehen – diese Ausgabe der *FIfF-Kommunikation* ist stark durch die vom Corona-Virus ausgelöste Krise geprägt. Neben der inhaltlichen Arbeit wird auch die Organisation des FIfF stark dadurch beeinflusst.

Ingrid Schlagheck und Philip Love von unserer Geschäftsstelle arbeiten derzeit verstärkt aus dem Home-Office und können dadurch den gewohnten Betrieb weitestgehend aufrechterhalten. Sie haben auch dafür gesorgt, dass diese Ausgabe der *FIfF-Kommunikation* ihre Leserinnen und Leser wie gewohnt erreicht hat – per Post und auf unserer Webseite. Vielen Dank dafür, das ist nicht selbstverständlich.

Wir vermissen die Konferenzen, persönlichen Begegnungen und Diskussionen, die sonst im Lauf des Jahres regelmäßig stattfinden. Einiges davon hat sich in die digitale Sphäre verlagert. Auch das funktioniert; es muss sich aber noch einiges einrütteln. Lasst uns die Digitalisierung als eine positive Entwicklung gestalten – aber stets im kritischen Bewusstsein, dass sie mit Risiken verbunden ist und nicht naiv übernommen werden sollte. Die Datenschutz-Folgenabschätzung, die wir zur Corona-App veröffentlicht haben, soll dabei einen wegweisenden Charakter haben – vielen Dank an alle, die daran mitgewirkt haben.

Besonders schmerzlich – und damit komme ich zum Anlass dieses Textes – ist, dass auch unsere FIfF-Konferenz in diesem Jahr betroffen sein wird. Anfang Februar traf sich der Vorstand in Weimar; voller Vorfreude auf die in dieser wunderschönen Stadt im November geplante Tagung fuhren wir am Sonntagnachmittag nach Hause. Doch heute gehen wir davon aus, dass wir bis ins nächste Jahr noch mit Einschränkungen wegen der Corona-Krise leben müssen und haben im Moment keine belastbare Planungsgrundlage. Auch andere wissenschaftliche Konferenzen werden in absehbarer Zeit virtuell stattfinden. Es ist nicht einmal abzusehen, welche Maßnahmen es in den kommenden Wochen und Monaten geben wird, falls es zu einer *second wave* der Pandemie kommen sollte.



Auch hier weist die Digitalisierung den Weg. Eine kurzfristige Absage oder gar die Infizierung von TeilnehmerInnen wollen wir nicht riskieren. Wir planen nun eine virtuelle Konferenz und untersuchen die Möglichkeiten, sie unter Berücksichtigung unserer Standards zu realisieren. Es ist damit das erste Mal in der Geschichte des FIfF, dass in einem Jahr keine FIfF-Konferenz vor Ort stattfindet. Gerade eine Konferenz, die sich thematisch im Spannungsfeld von IT-Sicherheit und Ergonomie – mit dem wichtigen Aspekt der Barrierefreiheit – bewegen soll, stellt bei der Digitalisierung besondere Herausforderungen.

Was am Ende dabei herauskommt, wissen wir selbst noch nicht. Aber wir arbeiten daran und freuen uns darauf. Wir erwarten, Euch auch in diesem Jahr ein spannendes FIfF-Ereignis präsentieren zu können.

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.